CYBERWEERBAARHEID

Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime

Kwetsbare doelgroepen en bijbehorende typen cyberdelicten

Geïntegreerd deelrapport werkpakketten 1 en 2

SIA Regieorgaan

COLOFON

Dit onderzoek is uitgevoerd door onderzoekers van het lectoraat Maatschappelijke Veiligheid van Hogeschool Saxion en het lectoraat Cybersecurity in het mkb van de Haagse Hogeschool:

Dr. Ellen Misana-ter Huurne[1]
Dr. Susanne van 't Hoff-de Goede[2]
Luuk Bekkers, MSc.2
Dr. Ynze van Houten[1]
Michelle Walther, MSc.[1]
Dr. Remco Spithoven[1]
Dr. Rutger Leukfeldt[23]

in samenwerking met de consortiumpartners binnen het project 'Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime':

Veiligheidsalliantie Regio Rotterdam
Noord-Holland Samen Veilig
Gemeente Almere
Gemeente Apeldoorn
Gemeente Den Helder
Gemeente Ede
Gemeente Haarlem
Gemeente Utrecht
Regionale Veiligheidsstrategie Midden-Nederland
Veiligheidsnetwerk Oost-Nederland
Gemeente Amersfoort
Gemeente Capelle a/d IJsse
Gemeente Dordrecht
Gemeente Enschede
Gemeente Rotterdam
Gemeente Zoetermeer
Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)

Dit onderzoek is medegefinancierd door Regieorgaan SIA, onderdeel van de Nederlandse organisatie voor Wetenschappelijk Onderzoek (NWO).

1 Hogeschool Saxion
2 De Haagse Hogeschool
3 Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)

VOORWOORD

"Cybercrime verdubbeld in jaar tijd. De politie zag in 2020 veel meer digitale misdrijven dan het jaar ervoor. Criminelen verleggen hun werkterrein van de fysieke wereld naar internet. Daar houden zich ook hun slachtoffers op: gewone burgers en bedrijven" kopte de Volkskrant op 15 januari 2021. Het is slechts één van de vele berichten die iedere dag in de media verschijnen ten aanzien van de groei van cybercriminaliteit in de laatste jaren. Dat cybercriminaliteit inmiddels geschaard kan worden onder de noemer veel voorkomende criminaliteit, moge duidelijk zijn. De aanpak ervan roept echter nog wel de nodige vraagtekens op. Want hoe spoor je op en handhaaf je in de digitale wereld, waarbij daders en slachtoffers letterlijk duizenden kilometers bij elkaar vandaan kunnen zitten? En wat is de rol van de lokale overheid bij de aanpak van deze veelvoorkomende vorm van criminaliteit?

In het project "Cyberweerbaarheid: Een gemeentelijk offensief ter voorkoming van slachtofferschap van cybercriminaliteit" geven we vorm aan een lokale aanpak van cybercriminaliteit. De hoofdvraag van het project is dan ook: hoe kunnen we inwoners en ondernemers helpen om te voorkomen dat zij slachtoffer worden en zichzelf zo goed mogelijk te beschermen tegen cybercriminaliteit? Om dat te kunnen bereiken, moet eerst antwoord gevonden worden op de vragen: wat zijn de meest kwetsbare doelgroepen en van welke typen delicten worden zij dan slachtoffer? Alleen op basis daarvan zullen we in staat worden gesteld om effectieve en doelgroepgerichte interventies te ontwikkelen ten behoeve van de cyberweerbaarheid. Deze vragen staan dan ook centraal in dit eerste deelrapport.

Dit onderzoek had niet uitgevoerd kunnen worden zonder de hulp van vele partijen. We bedanken iedereen die op welke wijze dan ook een bijdrage heeft geleverd aan dit onderzoek. Ten eerste alle consortiumpartners: dank voor jullie bijdrage aan de interviews en de nuttige discussies en input tijdens de consortiumbijeenkomsten. Ook dank voor het toetsen van de resultaten aan de lokale beroepspraktijk. Daarnaast bedanken we alle professionals en experts die bereid waren zich te laten interviewen en hun meest recente en waardevolle kennis met ons te delen op het gebied van slachtofferschap en typen cyberdelicten.

Ellen Misana-ter Huurne
Susanne van 't Hoff-de Goede
Luuk Bekkers
Ynze van Houten
Michelle Walther
Remco Spithoven
Rutger Leukfeldt

SAMENVATTING

Gezien de toenemende omvang en impact van cybercriminaliteit, vinden lokale overheden het van belang te zoeken naar manieren om deze vormen van criminaliteit te voorkomen of aan te pakken. In het project “Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime” werken professionals uit twaalf gemeenten en vier regionale veiligheidsnetwerken samen met onderzoekers aan het verhogen van de cyberweerbaarheid van de lokale samenleving. Het doel is om te komen tot beproefde interventies die lokale overheden kunnen inzetten om de cyberweerbaarheid onder inwoners en ondernemers binnen hun gemeente te vergroten. Om te komen tot effectieve interventies die ambtenaren openbare orde en veiligheid hiertoe in hun gemeente kunnen inzetten te vergroten, is de centrale doelstelling opgedeeld in subdoelen:

1. Het in kaart brengen van de meest kwetsbare doelgroepen
2. Het in kaart brengen van de vormen van cybercrime waarvan zij slachtoffer worden
3. Het inzichtelijk maken van de onderliggende factoren en verklaringen van hun risicobewustzijn
en preventieve gedrag ten aanzien van cybercrime.
4. Het ontwikkelen en implementeren van effectieve interventies die Nederlandse gemeenten kunnen inzetten om het risicobewustzijn en het preventieve gedrag rondom deze vormen cybercrime onder deze doelgroepen kunne bevorderen.

Dit rapport beschrijft de resultaten van de eerste twee deelvragen, te weten *1) Voor welke doelgroepen zijn interventies om het risicobewustzijn en het preventieve gedrag te vergroten het meest noodzakelijk?* en *2) Voor welke typen cybercrime zijn interventies om het risicobewustzijn en het preventieve gedrag van deze doelgroepen te vergroten het meest noodzakelijk?* Omdat doelgroepen en typen cyberdelicten vaak onlosmakelijk met elkaar verbonden zijn, is gekozen voor de geïntegreerde rapportage van deze twee onderzoeksvragen.

Op basis van een combinatie van onderzoeksmethoden van literatuurstudie en meerdere interviewrondes met gemeentelijke functionarissen en experts uit het werkveld van cybercriminaliteit is een actueel inzicht gegeven in de meest relevante doelgroepen en typen cyberdelicten waarvan zij slachtoffer worden.
Bij de beantwoording van de eerste onderzoeksvraag *“Voor welke doelgroepen zijn interventies om het risicobewustzijn en het preventieve gedrag te vergroten het meest noodzakelijk?”* is gebleken, dat op basis van de literatuurstudie geen eenduidig risicoprofiel voor meest kwetsbare groepen slachtoffers van cybercriminaliteit kan worden gedefinieerd. Studies zijn gericht op de samenhang tussen verschillende kenmerken en slachtofferschap, maar concludeerden dat er zeer beperkte samenhang tussen de afzonderlijke kenmerken als geslacht, opleidingsniveau en sociaal economische status en het risico op slachtofferschap van cybercriminaliteit te maken is. Toch zijn uit de literatuurstudie wel twee groepen naar voren gekomen die een verhoogd risico op slachtofferschap van cybercriminaliteit lijken te hebben: jongeren en mkb’ers (midden- en klein bedrijf). Jongeren lijken vooral een verhoogd risico te lopen op *interpersoonlijke cyberdelicten*, zoals stalking, bedreiging met geweld en laster. Mkb’ers lijken verhoogd risico te lopen op zowel *financiële* als *technische cyberdelicten*, zoals phishing, hacking en malware.

Daarnaast komen op basis van de resultaten van de interviews met zowel gemeentelijke functionarissen op het gebied van cybercriminaliteit als de overige experts uit het vakgebied, zoals politie, banken en kennisinstelligen, drie prominente doelgroepen in deze studie naar voren gekomen: **jongeren, ouderen** en **mkb’ers.**
Bij de beantwoording van de tweede onderzoeksvraag (*Voor welke typen cybercrime zijn interventies om het risicobewustzijn en het preventieve gedrag van deze doelgroepen te vergroten het meest noodzakelijk?*) is op basis van de literatuur een aantal delicten aangewezen als de meest voorkomende delicten en daarmee de delicten waarvoor het vergroten van cyberweerbaarheid bij potentiële slachtoffers het meest noodzakelijk is; binnen de *technische cyberdelicten* zijn dit hacking en malware; in de categorie *financiele cyberdelicten* aankoopfraude, phishing en identiteitsfraude en binnen de *interpersoonlijke delicten* zijn dit laster, chantage, stalking en bedreiging met geweld (al dan niet met een seksuele bijbedoeling).

Tijdens de interviews met vertegenwoordigers van gemeenten en experts in het veld van cybercriminaliteit en cyberweerbaarheid zijn verschillende delicten aangewezen als de meest prominente delicten om cyberweerbaarheid tegen te verhogen onder potentiële slachtoffers, zijnde: **phishing, shame sexting / sextortion, malware/ ransomware, vriend- in-noodfraude** en **geldezelen**.
Op basis van de keuze van de meest prominente doelgroepen en cyberdelicten is vervolgens op basis van de literatuur een inventarisatie gedaan van de meest prominente typen cyberdelicten binnen elke doelgroep. Voor de doelgroep jongeren komt de categorie *interpersoonlijke cyberdelicten* het

meest prominent naar voren. Bij de doelgroep mkb'ers komt met name de categorie *technische cyberdelicten* naar voren. Op basis van de resultaten uit de interviews komt een koppeling naar voren tussen ouderen en *financiële cyberdelicten*.
Vervolgens is gekeken of er een koppeling kon worden gemaakt tussen specifieke cyberdelicten en doelgroepen. De doelgroep jongeren werd het vaakst aan shame sexting / sextortion en geldezelen gekoppeld. Mkb'ers lopen volgens gemeenten en experts het meest risico op slachtofferschap van ransomware. Binnen de doelgroep ouderen kwam vooral vriend-in-nood fraude (Whatsapp-fraude) naar voren.
Naast de koppelingen tussen cyberdelicten en doelgroepen die naar voren gekomen zijn in deze studie, hebben diverse experts ook gewezen op prominente cyberdelicten die niet aan een specifieke doelgroep te koppelen zijn. Iedereen kan slachtoffer worden van dergelijke cyberdelicten.
De experts benadrukken dan ook het belang van het verbeteren van algemene cyberweerbaarheid onder internetgebruikers. Daarbij kan niet voorbij gegaan worden aan het meest prominente cyberdelict; phishing. Daar de resultaten erop wijzen dat voor phishing geen specifieke doelgroep aangewezen kan worden, is dit delict gekoppeld alle drie de doelgroepen.
Vervolgonderzoek binnen deze groepen is nodig om de vraag te beantwoorden waarom juist deze groepen vaker slachtoffer worden van cybercriminaliteit en welke verklarende factoren en motieven een rol spelen bij het risicobewustzijn, het zelfbeschermende gedrag en de cyberweerbaarheid van de doelgroepen met betrekking tot de specifieke delicten. Deze inzichten zijn noodzakelijk om te kunnen komen tot effectieve en doelgroepgerichte interventies die gemeenten kunnen inzetten om de cyberweerbaarheid in de lokale samenleving te vergroten. Deze vraag staat centraal in werkpakket 3, waar het doel is de onderliggende factoren en verklaringen van hun risicobewustzijn en preventieve gedrag ten aanzien van specifieke cyberdelicten per doelgroep inzichtelijk te maken door middel van kwantitatief en kwalitatief onderzoek onder deze doelgroepen.

INHOUDSOPGAVE

INLEIDING

1.1. Aanleiding

Ambtenaren openbare orde en veiligheid van gemeenten spelen een centrale rol in de zorg voor lokale maatschappelijke veiligheid. Hun focus ligt van oudsher op de preventie van slachtofferschap van high volume crime (zoals diefstal, vernielingen en vandalisme) en high impact crime (zoals woninginbraak, overvallen en straatroven) binnen hun verzorgingsgebied. Intussen heeft de digitalisering van de samenleving een ongeëvenaarde gelegenheid voor criminaliteit gecreëerd. Door de groei van het aantal (geregistreerde) cyberdelicten, hebben Nederlandse gemeenten in toenemende mate aandacht voor cybercriminaliteit in hun veiligheidsbeleid. Maar in de uitwerking van deze beleidsprioriteit in concrete interventies schuilt een grote uitdaging. Duidelijk is dat de ambtenaren openbare orde en veiligheid een taak voor zichzelf zien in de preventie van cybercriminaliteit, maar waar te beginnen?

Inmiddels wordt cybercriminaliteit bestempeld als een groot maatschappelijk probleem (Beerthuizen, Sipma, & Van der Laan, 2020). De online gelegenheid voor criminaliteit is groot, zeker in Nederland. Maar liefst 98% van onze bevolking is aangesloten op het internet, tegenover het Europese gemiddelde van 87% (Eurostat, 2018). Gezien de toenemende omvang en impact van cybercriminaliteit, is het van belang te zoeken naar manieren om deze vormen van criminaliteit te voorkomen of aan te pakken.
In het project "Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime" werken professionals uit twaalf[4] gemeenten en vier[5] regionale veiligheidsnetwerken samen met onderzoekers van de Haagse Hogeschool, Hogeschool Saxion en het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving (NSCR) aan bovengenoemd vraagstuk. Hierbij is het overkoepelende doel te komen tot (beproefde) effectieve interventies die lokale overheden kunnen inzetten om de cyberweerbaarheid binnen hun gemeente te vergroten. Cyberweerbaarheid in dit project is daarmee vooral gericht op de menselijke kant van de cybersecurity: het vergroten van het zelfbeschermend gedrag van burgers en ondernemers. Onder zelfbeschermend gedrag wordt in dit rapport verstaan: die acties of gedragingen die mensen uitvoeren om zichzelf te beschermen tegen risico's, gevaren of de gevolgen daarvan (inclusief (negatieve) emoties) (Spithoven, 2020). Juist bij het bevorderen hiervan is het belangrijk om inzicht te krijgen in de percepties, beleving, behoeftes en (risicovolle) gedragingen van de doelgroep. Het doel is immers om (groepen) individuen daadwerkelijk in staat te stellen en te stimuleren om zichzelf (beter) te beschermen. Hiervoor zijn een aantal aspecten belangrijk. Mensen moeten: (I) weten (risicobewustzijn); (II) willen (perceptie eigen verantwoordelijkheid); (III) kunnen (zelfeffectiviteit) en (IV) doen (gedrag) (Spithoven, 2020; Misana- ter Huurne, Van Houten, Spithoven, Notté, & Leukfeldt, 2020; Leukfeldt, Spithoven, & Misana-ter Huurne, 2020). Hiertoe wordt het Cyberweerbaarheidsmodel als theoretische basis gebruikt in dit project (zie Bijlage 1).
De hoofdvraag van dit project luidt: Met welke interventies kunnen ambtenaren

openbare orde en veiligheid de cyberweerbaarheid van burgers en bedrijven binnen hun gemeente vergroten?

1.2. Doelstelling

Om te komen tot effectieve interventies voor ambtenaren openbare orde en veiligheid om de cyberweerbaarheid binnen hun gemeente te vergroten, is de centrale doelstelling opgedeeld in subdoelen:

1. Het in kaart brengen van de meest kwetsbare doelgroepen;
2. Het in kaart brengen van de vormen van cybercriminaliteit waarvan zij slachtoffer worden;
3. Het inzichtelijk maken van de onderliggende factoren en verklaringen van hun risicobewustzijn en preventieve gedrag ten aanzien van cybercriminaliteit;
4. Het ontwikkelen en implementeren van effectieve interventies die Nederlandse gemeenten kunnen inzetten om het risicobewustzijn en het preventieve gedrag rondom deze vormen cybercriminaliteit onder deze doelgroepen kunnen bevorderen.

In dit deelrapport staan de eerste twee subdoelen centraal; 1) het in kaart brengen van vhet vergroten van de cyberweerbaarheid het meest urgent is, en 2) het in kaart brengen van de vormen van cybercriminaliteit waarvan zij het meeste slachtoffer worden. Op basis van zowel wetenschappelijke als praktijkkennis worden de drie meest urgente doelgroepen geïdentificeerd. Per doelgroep wordt inzichtelijk gemaakt van welke twee vormen van cyberdelicten zij het meest

slachtoffer worden. Hiermee wordt inzicht gegeven in de richting voor de te ontwikkelen interventies in de volgende werkpakketten om de cyberweerbaarheid te vergroten.

1.3. Onderzoeksvragen

Om te komen tot een overzicht van meest kwetsbare doelgroepen en vormen van cybercriminaliteit waarvan deze kwetsbare doelgroepen het meest slachtoffer worden, staan daarom de volgende onderzoeksvragen centraal in dit deelrapport:

1. Voor welke doelgroepen zijn interventies om het risicobewustzijn en het preventieve gedrag te vergroten het meest noodzakelijk?

2. Voor welke typen cybercrime zijn interventies om het risicobewustzijn en het preventieve gedrag van deze doelgroepen te vergroten het meest noodzakelijk?

De resultaten van dit deelproject vormen het vertrekpunt voor de volgende fase, waarin onderzocht wordt hoe het is gesteld met het risicobewustzijn en het preventieve gedrag onder deze doelgroepen met betrekking tot deze vormen van cybercriminaliteit, en welke bepalende factoren hieraan ten grondslag liggen.

1.4. Leeswijzer

Dit rapport start in Hoofdstuk 2 met een uiteenzetting over de focus op cyberweerbaarheid als instrument om het slachtofferschap en de impact van cybercriminaliteit te minimaliseren. In Hoofdstuk 3 worden de onderzoeksmethoden toegelicht. Vervolgens worden in de hoofdstukken 4 en 5 de resultaten beschreven, waarbij in Hoofdstuk 4 de resultaten van de literatuurstudie centraal staan en in Hoofdstuk 5 de resultaten van de gehouden interviews. Hoofdstuk 6 bevat de conclusie en discussie. Hierin worden de onderzoeksvragen beantwoord en aanbevelingen gegeven wat betreft de doelgroepen en bijbehorende vormen van cybercriminaliteit die in de volgende onderzoeksfasen centraal staan.

4 Almere, Amersfoort, Apeldoorn, Capelle a/d IJssel, Den Helder, Dordrecht, Ede, Enschede, Haarlem, Utrecht, Rotterdam, Zoetermeer.

5 VeiligheidsAlliantie Rotterdam, Veiligheidsnetwerk Oost-Nederland, Noord-Holland Samen Veilig, Regionale Veiligheidsstrategie Midden-Nederland.

2. FOCUS OP CYBERWEERBAARHEID

Dit hoofdstuk schetst de rol van en focus op 'cyberweerbaarheid' om (de effecten van) cybercriminaliteit voor eindgebruikers tegen te gaan of te minimaliseren. Hierbij wordt ingegaan op het belang van doelgroepgerichte risicocommunicatie-interventies om zelfbeschermend gedrag te stimuleren als instrument voor het verhogen van de cyberweerbaarheid van eindgebruikers.

2.1. Cyberweerbaarheid

Harde cijfers ontbreken, maar experts schatten dat ongeveer 95% van alle succesvolle cyberdelicten hun oorsprong vinden in menselijk handelen (onveilig gedrag, gebrek aan kennis en vaardigheden, ontbreken van richtlijnen of het niet naleven van gedragsregels) (Roelofs e.a., 2018). De mens wordt daarmee bestempeld als de zwakste schakel in de prevalentie van cybercriminaliteit (Ceesay e.a., 2018). De winst om deze delicten in de kiem te smoren ligt daarmee niet alleen in het opsporen van daders of technologische faciliteiten, maar juist ook in het vergroten van de weerbaarheid van potentiële slachtoffers van cyberdelicten (Munnichs, Kouw, & Kool, 2017; Jansen, 2018). Daarmee richt cyberweerbaarheid zich in dit project op de menselijke kant van de cybersecurity: preventie van slachtofferschap en schade door het stimuleren van het risicobewustzijn en veilig online gedrag van eindgebruikers. Met andere woorden: het vergroten van de cyberweerbaarheid.
Cyberweerbaarheid is een term die steeds vaker wordt beschreven in de literatuur over de aanpak van cybercriminaliteit, maar een eenduidige definitie ontbreekt tot op heden. Björk e.a. (2015) definiëren het als het vermogen om continu de beoogde resultaten te kunnen leveren ondanks ongunstige cyber 'events'. Het Nationaal Cyber Security Centrum (2016) definieert cyberweerbaarheid als de mogelijkheid om gebruik te maken van ICT zonder het risico of de kans om daarbij geraakt te worden door schade. Hierbij gaat het niet alleen om (opzettelijk) misbruik, maar worden ook de risico's door verstoring, uitval of beperkte beschikbaarheid van ICT meegenomen. Spithoven (2020) en Misana-ter Huurne e.a. (2020) definiëren het als *'De combinatie van een voldoende hoge mate van risicobewustzijn en zelfbeschermend gedrag onder burgers en ondernemers om slachtofferschap van cybercriminaliteit te voorkomen en/of mogelijke impact te voorkomen of verkleinen.'* Toegepast op het huidige onderzoek, wordt cyberweerbaarheid benaderd vanuit de gedragingen of acties die iemand neemt om zichzelf te beschermen tegen deze cyberrisico's of de gevolgen daarvan, gebaseerd op het risicobewustzijn en bijbehorende verklarende factoren van gedrag. Het betreft daarmee de mate waarin iemand in staat is tegenstand te bieden tegen cybercriminaliteit, ofwel zelfbeschermend gedrag te vertonen met betrekking tot cybercriminaliteit (Jansen, 2018; Van der Kleij en Leukfeldt, 2019).

2.2. Cyberweerbaarheidsverhoging door doelgroepgerichte risicocommunicatie

Daarmee ligt er een maatschappelijke uitdaging in het bevorderen van dit gedrag om slachtofferschap van cybercriminaliteit te voorkomen. Want het gedrag van eindgebruikers staat aan de basis van het al dan niet slagen van een poging tot cybercriminaliteit (Leukfeldt, 2018). Burgers en bedrijven moeten in staat worden gesteld om hun gedrag aan te passen en daarvoor is het nodig te weten hoe en waarom zij dat moeten doen. Uit eerder onderzoek is gebleken dat effectieve risicocommunicatie en voorlichting een stevige bijdrage leveren aan het preventief gedrag van eindgebruikers en daarmee hun capaciteit om zichzelf of hun organisatie te beschermen tegen de mogelijke risico's en effecten van cybercriminaliteit (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010).
Risicocommunicatie is echter meer dan het verschaffen van informatie over risico's en gevolgen. Juist bij het bevorderen van preventief gedrag speelt risicocommunicatie een rol die verder gaat dan louter informeren (Kievik e.a., 2018; ter Huurne, 2008). Algemene, massamediale campagnes zijn onvoldoende in staat om daadwerkelijk gedrag te beïnvloeden (Renes e.a., 2011). Risicocommunicatie is maatwerk. Het is van belang om de communicatie over cybercriminaliteit persoonlijk relevant en dichtbij te maken, zodat individuen de neiging hebben om hun gedrag aan te passen. Dit vraagt om bottom-up communicatie: allereerst het inzichtelijk maken van de behoeften, beleving, percepties en overtuigingen van de doelgroep, waaruit verklaringen gevonden kunnen worden voor welke factoren bepalend zijn voor het wel of niet uitvoeren van zelfbeschermend gedrag. Op basis hiervan kunnen dan effectieve, doelgroepgerichte interventies ontwikkeld worden, die daadwerkelijk aansluiten bij de beleving en behoeftes van de doelgroep, waardoor de effectiviteit vergroot wordt (Griffin e.a., 1999; Ter Huurne, 2008; Kievik e.a., 2018). We vragen immers iets van de ontvanger; we willen dat hij of zij het eigen gedrag gaat aanpassen. Risicocommunicatie is daarmee in essentie bedoeld om individuen te ondersteunen om geïnformeerde beslissingen te nemen ten aanzien van de risico's waarmee zij worden geconfronteerd; of zoals Wade en collega's het beschreven: "The purpose of risk communication is to assist people to make informed choices about the risks they face in daily life" (Wade e.a., 1992).
Bij het ontwikkelen van effectieve interventies om gedragsverandering te stimuleren, is een aantal aspecten belangrijk. Risicocommunicatieboodschappen om gedragsverandering te stimuleren zijn het meest effectief wanneer zij enerzijds inspelen op het verhogen van de risicoperceptie en anderzijds het aanbieden van concrete, als makkelijk uitvoerbaar en nuttig ervaren, gedragsadviezen (ter Huurne, 2008; Kievik e.a., 2018). De sleutel bij risicocommunicatie ligt in het denken in doelgroepen in combinatie met het geven van concrete handelingsperspectieven. Deze laatste variëren per type delict (om te voorkomen dat je gehackt wordt, moet je andere

voorbereidingsmaatregelen treffen dan bij het voorkomen van identiteitsfraude). Elke doelgroep vraagt om een op maat gemaakte

aanpak en deze start bij het achterhalen en verklaren van het risicobewustzijn en het preventieve gedrag rondom het specifieke risico onder de doelgroep. Op deze wijze kan risicocommunicatie een bijdrage leveren aan het preventieve gedrag van eindgebruikers en daarmee hun capaciteit om zichzelf en/of hun organisatie te beschermen tegen mogelijke risico's en negatieve effecten (Sheng, e.a., 2010).
Kennis over hoe Nederlanders zich online gedragen en hoe zij zich (kunnen) weren tegen online criminaliteit is echter nog beperkt (Van 't Hoff- de Goede e.a., 2019). Voor het ontwikkelen en onderbouwen van effectieve interventies gericht op (zelfbeschermend) gedrag is inzicht hierin onontbeerlijk. Daarmee is de eerste stap het inzichtelijk maken van de kwetsbare doelgroepen en de typen cyberdelicten, om van daaruit gedragingen, specifiek dan wel geclusterd, in kaart te brengen die geassocieerd zijn met een verhoogd risico op slachtofferschap én de impact daarvan.

2.3. Kwetsbare doelgroepen en typen cyberdelicten

Het definiëren van kwetsbare doelgroepen is een uitdaging. Vaak wordt gekeken naar welke doelgroepen de meeste *kans* maken om slachtoffer te worden en welke factoren daaraan bijdragen. De kans op slachtofferschap kan vergroot worden door bijvoorbeeld bepaalde gedragingen of de hoeveelheid tijd die men online besteedt. Echter, een specifieke gedraging hangt niet altijd samen met een specifieke vorm van slachtofferschap; het klikken op een phishing-link, bijvoorbeeld, kan leiden tot onder meer financieel verlies of een ransomwarebesmetting (zie bijvoorbeeld Van 't Hoff-de Goede e.a., 2019). Het is dus moeilijk kwetsbare groepen te identificeren op basis van kansinschatting alleen; alle internetgebruikers zijn potentiële slachtoffers (Leukfeldt, 2014; Leukfeldt, 2015; Van 't Hoff-de Goede e.a., 2019; Bossler & Holt, 2009; Veenstra e.a., 2015; Sipma & Van Leijsen, 2019).
Daarmee is kans op slachtofferschap in dit onderzoek niet de enige variabele waarmee rekening gehouden wordt. Ook de *impact* die slachtofferschap kan hebben op verschillende doelgroepen weegt mee in de overweging om de mate van kwetsbaarheid vast te stellen. De omvang of ernst van de gevolgen die slachtofferschap kan hebben op het leven, kan namelijk per doelgroep, maar ook per type delict variëren. Daarom wordt deze factor ook nadrukkelijk meegenomen in dit onderzoek bij het identificeren van relevante kwetsbare doelgroepen.
Naast de verschillende factoren die slachtofferschap beïnvloeden, is ook het aantal verschillende typen cyberdelicten is zeer groot en divers. Om hier op gestructureerde wijze inzicht in

te verkrijgen, worden de delicten die aan bod komen in drie hoofdcategorieën[6] opgedeeld (cf. Leukfeldt e.a., 2015), te weten:

1. Cybercriminaliteit gericht op computers (technische cyberdelicten)

Bij dit type delict is de computer of website niet alleen het middel om het delict te plegen, maar ook het doelwit. Bijvoorbeeld het inbreken in computers (hacken) het vernielen van digitale bestanden of het stelen van gegevens.

2. Cybercriminaliteit met een financieel oogmerk (financiële cyberdelicten)

Bij dit type delict is het doel van de dader financieel gewin. Het kan gaan om klassieke delicten zoals oplichting waarbij gebruik is gemaakt van internet, maar ook om phishing of verkoopfraude.

3. Persoonsgerichte cybercriminaliteit (interpersoonlijke cyberdelicten)

Dit type delict wordt vaak aangeduid als interpersoonlijke delicten. Het gaat om digitale vormen van strafbare gedragsdelicten waarbij de persoonlijke levenssfeer wordt aangetast. Hierbij maken daders gebruik van ICT als (eenzijdig) communicatiemiddel richting het slachtoffer. Voorbeelden zijn bedreiging, stalking en laster.

6 Een vierde categorie, genaamd 'Kinderporno en andere zedendelicten' (Leukfeldt e.a. (2015)) valt buiten de scope van dit project en wordt om die reden niet meegenomen in dit rapport. Interpersoonlijke delicten met een seksuele bijbedoeling (zoals sextortion) worden echter wel meegenomen in dit onderzoek en ondergebracht in de categorie 'Interpersoonlijke cybercriminaliteit').

3. ONDERZOEKSOPZET

De onderzoeksvragen in dit rapport zijn van verkennende aard en hebben als doel om een actueel inzicht te geven in de meest relevante doelgroepen en typen cyberdelicten waarvan zij slachtoffer worden. Om die reden is een combinatie van onderzoeksmethoden ingezet, te weten (I) literatuurstudie en (II) interviews. Aanvullend zijn discussiebijeenkomsten georganiseerd met de praktijkpartners om de inzichten te toetsen aan hun beleidsvisies en kritisch te reflecteren op de bevindingen.

3.1. Literatuurstudie

In de literatuurstudie werd gebruik gemaakt van bestaande onderzoeksgegevens, waarbij de focus in dit project vooral ligt op het onderzoeken van overheids- en wetenschappelijke bronnen. Met overheidsbronnen worden de meest recente numerieke overzichten en rapporten van politie, (openbaar) ministerie, onderzoeksinstellingen en gemeenten over slachtofferschap van cybercriminaliteit bedoeld. Met wetenschappelijke bronnen worden officiële publicaties in wetenschappelijke tijdschriften (peer-reviewed) en gepubliceerde onderzoeksrapporten van wetenschappelijke onderzoeksinstellingen bedoeld.
Alvorens potentiële bronnen op inhoud zijn bestudeerd, zijn deze op de gangbare kwaliteitseisen[7] voor literatuurstudie gewogen. Wanneer dit leidde tot het oordeel dat het materiaal bruikbaar is voor de beantwoording van de deelvraag, werd over gegaan tot de analyse van de inhoud. De daadwerkelijke inhoudsanalyse van deelvraag 1 vindt plaats aan de hand van de volgende inhoudelijke aspecten: (I) Wordt er in de presentatie van de aantallen (geschatte) slachtoffers onderscheid in potentiële doelgroepen gemaakt?; (II) Wat zijn de (geschatte) aantallen slachtoffers per doelgroep? Bij deelvraag 2 vindt de analyse plaats aan de hand van de volgende inhoudelijke aspecten: (I) Wordt er in de presentatie van de aantallen (geschatte) slachtoffers onderscheid in verschillende typen cybercriminaliteit gemaakt?; (II) Wat zijn de (geschatte) aantallen slachtoffers per type cybercriminaliteit?

3.2. Interviews

De inzichten op basis van deskresearch worden aangevuld met interviews. Het doel is om hiermee actuele kennis en inzichten uit de praktijk op te halen. De ontwikkelingen bij cybercriminaliteit gaan snel en de wetenschappelijke literatuur is niet altijd up-to-date met betrekking tot de laatste ontwikkelingen. Daarnaast zijn praktijkinzichten relevant om inzicht te geven in de (lokale) ontwikkelingen van cybercriminaliteit in Nederland. Hierbij is gekozen voor een tweetrapsstrategie: In de eerste ronde zijn interviews gehouden met gemeentelijke functionarissen (N=12) met als doel inzicht te krijgen in de volgens hen meest relevante doelgroepen en typen cybercriminaliteit voor het verhogen van de cyberweerbaarheid. In de tweede ronde zijn interviews afgenomen met andere professionele deskundigen (N=16), zoals beleidsadviseurs, CEO's en cybercrime-analisten die op basis van hun kennis, ervaring en expertise indicaties kunnen geven van de omvang van slachtofferschap, kwetsbare doelgroepen, de meest voorkomende vormen van cybercriminaliteit en mogelijke trends en ontwikkelingen. Aanvullend zijn de resultaten van de twee interviewrondes getoetst aan de kennis en inzichten van lokale partners van de deelnemende gemeenten die in hun dagelijkse praktijk werken met de betreffende doelgroepen die naar voren kwamen. De gemeentelijke consortiumpartners hebben met behulp van een korte vragenlijst (Bijlage 4) de bevindingen uit de interviews voorgelegd aan deze praktijkpartners om te verifiëren of zij de prominente doelgroepen en bijbehorende delicten waarvan zij slachtoffer worden, herkennen in hun dagelijkse werk met deze doelgroepen. Tevens hebben zij aanvullende praktijkinzichten opgegeven over hoe deze doelgroepen het beste te bereiken zijn met interventies. Op deze wijze is een zo volledig en actueel mogelijk beeld geschetst van de huidige situatie omtrent doelgroepen en typen cybercriminaliteit.

3.2.1. Respondenten

In de eerste ronde zijn interviews gehouden met vertegenwoordigers van de twaalf deelnemende Nederlandse gemeenten. Respondenten zijn geselecteerd op basis van hun functieprofiel; zij zijn óf in dienst als ambtenaar openbare orde en veiligheid óf vervullen een functie die specifiek gericht is op cybercriminaliteit of cyberweerbaarheid voor de betreffende gemeente.
De twaalf deelnemende gemeenten zijn afkomstig uit zes verschillende provincies in Nederland, waarbij er een oververtegenwoordiging is van de grote gemeenten. Qua inwonertal zijn er twee gemeenten uit het segment 50.000-100.000 inwoners, drie uit het segment 100.000-150.000 inwoners, vier uit het segment 150.00-200.000 inwoners, en drie uit het segment groter dan 200.000 inwoners.Alle respondenten vertegenwoordigen een gemeente die cybercriminaliteit en/of cyberweerbaarheid heeft opgenomen in hun veiligheidsbeleid als aandachtspunt. Bij vier gemeenten was er sprake van een dubbel-interview[8].
In de tweede ronde zijn zestien interviews gehouden met deskundigen van publieke en private organisaties (anders dan gemeenten). Respondenten zijn geselecteerd op basis van hun kennis en werkzaamheden gerelateerd aan de preventie en aanpak van cybercriminaliteit of nazorg van slachtoffers. Op basis van de inzichten uit de eerste ronde interviews en een voorlopige selectie van doelgroepen, zijn respondenten geselecteerd op expertise over 1) slachtofferschap van specifieke delicten en/of binnen specifieke doelgroepen en/of 2) slachtofferschap en ontwikkelingen op het gebied van cybercriminaliteit in zijn algemeenheid.
Deze expert-respondenten zijn beschouwd als respondent voor één of beide onderzoeksvragen. Zo zijn zeven experts specifiek gespecialiseerd in een bepaalde doelgroep en hebben daarom beperkt zicht op andere slachtoffergroepen van cybercriminaliteit. Zij worden dan ook niet meegerekend als expert op het gebied van slachtoffergroepen (onderzoeksvraag 1). Eén expert richt zich specifiek op een bepaalde vorm van cybercriminaliteit en heeft derhalve beperkte expertise over andere typen cybercriminaliteit (onderzoeksvraag 2). De overige respondenten zijn vanwege de aard van hun werk en expertise aan te merken als expert voor

7 Dit betreft relevantie (niveau, vorm en actualiteit) en betrouwbaarheid (autoriteit, juistheid, objectiviteit en controleerbaarheid); ook wel de CRAAP-test genoemd (Currency, Relevance, Authority, Accuracy, Purpose).

zowel slachtoffergroepen (onderzoeksvraag 1) als typen cybercriminaliteit (onderzoeks vraag 2). Dit betekent dat er negen experts zijn geïnterviewd op het gebied van slachtoffergroepen en vijftien experts op het gebied van typen cybercriminaliteit.
Tabel 1 bevat een overzicht van de respondenten.

Respondentcode	Organisatie	Functie	Expert slachtoffergroepen (ozv1) (N=9)	Expert typen cybercrime (ozv 2) (N=15)
EXP1	Politie	Analist	X	X
EXP2	Politie	Projectleider	X	X
EXP3	Reclassering	Medewerker casuïstiek cybercriminaliteit	X	X
EXP4	Bank	Analist	X	X
EXP5	Bank	Veiligheidsadviseur	X	X
EXP6	Fraudehelpdesk	Communicatie-medewerker	X	X
EXP7	Cybersecurity-bedrijf	CEO		X (binnen doelgroep mkb)
EXP8	NCSC	Onderzoeker en adviseur		X (binnen doelgroep mkb)
EXP9	Slachtofferhulp	Beleidsmedewerker	X	X
EXP10	MKB-NL	Beleidsmedewerker		X (binnen doelgroep mkb)
EXP11	VNO-NWC	Regiomanager		X (binnen doelgroep mkb)
EXP12	Mediawijsheid	Strategischadviseur		X (binnen doelgroep jongeren)
EXP13	Politie	Teamleider	X (binnen de vorm aan- en verkoopfraude)	
EXP114	Helpwanted	Hulplijn medewerker		X (binnen doelgroep jongeren)
EXP15	KBO-PCOB	Beleidsadviseur		X (binnen doelgroep ouderen)
EXP16	Consumentenbond	Beleidsadviseur		X (binnen doelgroep ouderen)

8 Een 'dubbel-interview' houdt in dat van één gemeente twee functionarissen tegelijkertijd zijn geïnterviewd. In deze gemeenten is de uitvoering van cybercrime-gerelateerde werkzaamheden bij verschillende functionarissen belegd. Door deze gezamenlijk te interviewen, is een zo volledig mogelijk beeld ontstaan van de werkwijze met betrekking tot cybercrime in de betreffende gemeenten. Dergelijke dubbel-interviews zijn als één interview geteld.

3.2.2. Interviewvragen

De interviewleidraad is tot stand gekomen op basis van deskresearch en suggesties van zowel experts als onderzoekers. Hierbij zijn de onderzoeksvragen als vertrekpunt genomen. Er is gekozen voor een semigestructureerde aanpak. De vragen zijn vooral open vragen zodat respondenten vrij worden gelaten om de meest belangrijke aspecten eruit te lichten (in plaats van de interesses van de onderzoekers te volgen). Daarnaast biedt deze aanpak ook de mogelijkheid om door te vragen door de interviewer, waarbij ook dieper ingegaan kan worden op achterliggende overtuigingen of motieven.
De volledige vragenlijst gebruikt voor de interviews met de vertegenwoordigers van de gemeentes is bijgevoegd in Bijlage 2. De vragenlijst gebruikt bij de interviews met de experts (Bijlage 3) is deels overlappend met de vragenlijst gebruikt bij de gemeenten, en deels ingegeven door de resultaten uit de analyse van de gemeente-interviews. Daarmee zijn de uitkomsten van die analyse voorgelegd aan de experts om deze te toetsen en aanvullende inzichten te verwerven. In dit deelrapport worden alleen de resultaten van de analyses van de vragen uit de vragenlijst opgenomen die betrekking hebben op de onderzoeksvragen die centraal staan in dit deelrapport (vragen 4, 5, 7 en 8 uit Bijlage 2 en vragen 4, 5, 7, 10, 11, 12 en 13 uit Bijlage 3).

3.2.3. Procedure en analyse

De interviews zijn uitgevoerd door vijf onderzoekers van De Haagse Hogeschool en Hogeschool Saxion. De eerste interviewronde met de gemeenten vond plaats in de periode juni-augustus 2020. De interviews met de experts vonden plaats in november 2020. Door de maatregelen als gevolg van de coronacrisis zijn de interviews allemaal via online videogesprekken uitgevoerd. Van alle interviews zijn met toestemming van de respondent geluidsopnames gemaakt. Deze opnames zijn getranscribeerd door een professionele transcriptiedienst, waarna het geluidsfragment direct van de opnameapparatuur is verwijderd en de transcripten zijn geanonimiseerd. Op deze wijze is de benodigde anonimiteit, diepgang en accuraatheid van het proces geborgd.
De transcripten zijn vervolgens met behulp van ATLAS.ti[9] geanalyseerd. Bij het analyseren van de interviewtranscripten zullen we aan de hand van Saldaña (2012) en Frieze (2014) de volgende

9 ATLAS.ti is software gericht op de analyse van kwalitatieve onderzoeksgegevens.

stappen doorlopen:
Stap 1 Open coderen van de eerste tien interviews.
Stap 2 Terugbrengen van alle codes tot een eenduidige lijst. Deze lijst vormt de basis van het codeboek.
Stap 3 Coderen van de resterende transcripten aan de hand van het codeboek en nieuwe codes toevoegen.
Stap 4 Alle gecodeerde transcripten controleren op uniformiteit.
Stap 5 Controle op intersubjectiviteit: een andere onderzoeker checkt de gecodeerde transcripten aan de hand van het codeboek.

Hierbij zijn de transcripten gecodeerd op basis van de interviewvragen en zijn alle codes die benodigd zijn om de onderzoeksvragen te kunnen beantwoorden geselecteerd en gezamenlijk geanalyseerd. Op deze wijze zijn de verschillende, potentiële doelgroepen en de eigenschappen rondom slachtofferschap van cybercriminaliteit die gemeenten en experts aan hen toekennen in een analysematrix samengebracht door de onderzoekers. Hierdoor kan een tweede ranglijst worden opgesteld, waarbij - evenals bij de literatuurstudie - potentiële doelgroepen met een grote (geschatte) omvang van slachtofferschap van cybercriminaliteit bovenaan de ranglijst komen te staan, en potentiële doelgroepen met een lage (geschatte) omvang van slachtofferschap van cybercriminaliteit onderaan de ranglijst. Meerdere onderzoekers hebben dezelfde analyse van de gecodeerde transcripten gedaan om de betrouwbaarheid van de resultaten te waarborgen.
De onderzoeksvragen worden uiteindelijk beantwoord door de eerste ranglijst op basis van de literatuurstudie en de tweede ranglijst op basis van de interviews te combineren. Er worden hierbij twee tot drie doelgroepen aangewezen, en binnen elke groep maximaal twee delicten waarvan zij het meest slachtoffer lijken te worden. Dit betreffen de meest noodzakelijke doelgroepen en delicten om cyberweerbaarheid voor te verhogen. Dit resulteert in een onderbouwde keuze voor combinaties van doelgroepen en typen cyberdelicten waarvoor het verhogen van de cyberweerbaarheid het meest urgent is.

3.3. Discussiebijeenkomsten

In dit deelproject zijn twee discussiebijeenkomsten georganiseerd met alle consortiumpartners. De eerste vond plaats bij de start van het onderzoek op 11 februari 2020. Het doel van deze bijeenkomst met 27 deelnemers was om een eerste verkenning te doen van de ideeën, behoeftes en vragen over en reeds lopende initiatieven op het gebied van cyberweerbaarheid bij de deelnemers.
De tweede bijeenkomst met 25 deelnemers vond plaats op 12 november 2020[10] nadat de inzichten en resultaten van de literatuurstudie en interviews gereed waren. Hier was het bediscussiëren van en kritisch reflecteren op de resultaten en het bereiken van consensus over de implicaties voor de focus van de volgende werkpakketten. In twee workshoprondes is inhoudelijk gereflecteerd op de eerste resultaten uit de literatuurstudie en de interviews, waarbij ingegaan is op de geselecteerde doelgroepen en bijbehorende typen cyberdelicten waarvoor het verhogen van de cyberweerbaarheid het meest noodzakelijk is. Op deze wijze is continu aansluiting gezocht tussen de (bredere) onderzoeksresultaten en de praktijkbehoeftes van lokale overheden.

10 In verband met de coronamaatregelen heeft deze bijeenkomst online plaatsgevonden

4. INZICHTEN UIT DE LITERATUUR

In dit hoofdstuk worden de deelvragen die centraal staan in dit rapport beantwoord op basis van inzichten uit de literatuur. Daarbij wordt ingezoomd op de Nederlandse situatie en wordt op basis van de meest recente cijfers en onderzoeksresultaten beschreven welke doelgroepen en cyberdelicten het meest prominent naar voren komen in de cijfers. Dit wordt aangevuld met inzichten uit wetenschappelijke literatuur.
In paragraaf 4.1 zal eerst het meten van de prevalentie van cybercriminaliteit worden toegelicht. In 4.2 worden de meest voorkomende cyberdelicten besproken. Hierbij wordt de volgende indeling van cyberdelicten aangehouden, in lijn met eerdere studies: technische, financiële en interpersoonlijke cyberdelicten. Belangrijk is het om hierbij op te merken dat in de praktijk zaken door elkaar kunnen lopen en cyberdelicten uit meerdere categorieën samen kunnen komen. Zo kan een hack (technisch delict) bedoeld zijn om intieme foto's van een bekende te stelen (interpersoonlijk) om vervolgens geld af te dwingen (financieel). In paragraaf 4.3 wordt vervolgens onderzocht wie slachtoffer wordt van cyberdelicten en worden doelgroepen geïdentificeerd. Als deelconclusie volgt in 4.4 tot slot een koppeling tussen de meest voorkomende cyberdelicten en de meest prominente slachtoffergroepen.

4.1. Hoe vaak komt cybercriminaliteit voor in Nederland?

Hoeveel cyberdelicten jaarlijks in Nederland voorkomen kan worden bepaald aan de hand van politiegegevens en zelfrapportage onder slachtoffers. Uit deze bronnen komt een verschillend beeld naar voren. Zo wijzen zelfrapportage cijfers op slachtofferschap van cybercriminaliteit bij zo'n 10% van de Nederlandse bevolking in 2019, maar laten politiecijfers slechts 4700 cyberdelicten in Nederland in 2019 zien. De totstandkoming van deze cijfers en waarom ze ver uit elkaar liggen zal hier worden toegelicht.
Recente studies onder grote groepen Nederlanders hebben laten zien dat zo'n 10-13% van de Nederlanders in het afgelopen jaar[11] slachtoffer is geworden van een of meerdere cyberdelicten (CBS, 2019; CBS, 2020b; Sipma & Van Leijsen, 2019; Van 't Hoff-de Goede e.a., 2019) (zie Beerthuizen e.a., (2020) voor een overzicht). Het CBS (2020b) rapporteerde 13% online slachtofferschap in 2019, een percentage dat iets hoger ligt dan in 2017 (11%) en 2012 (12%). Het CBS includeert echter cyberpesten in deze cijfers, maar dit is niet in alle gevallen een strafbaar feit (Leukfeldt e.a., 2015). Om die reden zijn deze cijfers minder goed bruikbaar om een goed beeld te schetsen van de omvang van strafbare cyberdelicten.
Met aftrek van cyberpesten[12] blijft ongeveer 10% slachtofferschap in 2019 over. Dit is in lijn met de prevalentie van slachtofferschap van cybercriminaliteit die in andere studies werd gevonden. Zo rapporteerde Van 't Hoff-de Goede e.a. (2019) een percentage van 13%, waarbij geen interpersoonlijke delicten in acht zijn genomen.

11 Het jaar voorafgaand aan deelname van de betreffende studie.
12 Slachtofferschap van cyberpesten was in 2019 4,2 procent (CBS, 2020b). Hieronder vallen zowel strafbare delicten als stalking en bedreiging (1%) als niet strafbare gedragingen (zoals roddelen).

Op basis van het LISS-panel[13] ligt de omvang van cybercrime op bijna 10%, waarvan circa 2% bestaat uit online bedreigingen, waarbij mogelijk ook niet- strafbare incidenten zijn opgenomen (Sipma & Van Leijsen, 2019).

Zelfs bij deze hoge prevalentie van slachtofferschap in Nederland, moet rekening geworden houden met het feit dat cijfers op basis van zelfrapportage onder Nederlanders een onvolledig beeld laten zien. Een reden hiervoor is bijvoorbeeld dat mensen niet altijd weten dat ze slachtoffer zijn, zoals in het geval van het stelen van persoonsgegevens en malware. Ook is slachtofferschap mogelijk hoger in populaties die minder vaak meedoen aan slachtofferschaponderzoeken. Er zijn verschillende redenen dat slechts een beperkt deel van deze delicten terug komt in politiecijfers. Ten eerste is er onder slachtoffers sprake van een lage meldings- en aangiftebereidheid (Jong, Leukfeldt, & Van de Weijer, 2018; Van de Weijer e.a., 2020). Wanneer slachtoffers van cybercriminaliteit wel aangifte doen, worden deze bovendien niet altijd als zodanig geregistreerd bij de politie. Terwijl de politie openbaar maakte dat er in 2019 64 procent meer aangiftes van cybercriminaliteit dan in 2018 gedaan werden, en dat 4700 cyberdelicten werden geregistreerd (Politie, 2020a; 2020b), heeft dit alleen betrekking op delicten die enkel met internet gepleegd kunnen worden[14], zoals hacking en ransomware. Andere delicten, zoals online verkoopfraude, worden veelal niet als cybercriminaliteit aangemerkt. Dat er in mei 2020 meer cyberdelicten (1869) dan woninginbraken (1344) werden geregistreerd door de politie was nieuwswaardig, maar dit is slechts het topje van de ijsberg wanneer ook andere soorten online criminaliteit en niet-gemelde delicten (iets dat bij bijvoorbeeld woninginbraak veel minder voorkomt) in ogenschouw worden genomen. Met behulp van textmining is bijvoorbeeld geschat dat tussen de 132.000-293.000 registraties in 2016 betrekking hebben op gedigitaliseerde criminaliteit en tussen de 4000-25.000 op cybercriminaliteit (Tollenaar e.a., 2019)

4.2. Welke cyberdelicten komen het meest voor?

In de vorige paragraaf zijn de verschillende vormen van cybercriminaliteit uiteen gezet. In deze paragraaf worden de meest voorkomende vormen van cybercriminaliteit besproken. Hierbij wordt ingegaan op wat precies onder de verschillende delicten wordt verstaan en hoe vaak ze de afgelopen jaren zijn voorgekomen in Nederland. De delicten worden daarbij ondergebracht in drie categorieën: technische, financiële en interpersoonlijke cyberdelicten.

4.2.1. Technische cyberdelicten

Technische cyberdelicten zijn delicten waarbij IT niet alleen het middel is om het delict te plegen, maar ook het doelwit. Vaak zijn technische cyberdelicten een middel om een ander doel te bereiken, zoals het stelen, verwijderen of veranderen van informatie, documenten of geld.

13 Het LISS-panel is een bevolkingsonderzoek waarbij een vaste groep personen wordt gevolgd door de tijd heen.

14 Ook wel genoemd cybercriminaliteit in enge zin. Deze delicten worden bovendien bij de Politie geregistreerd onder de noemer “cybercriminaliteit”, zonder dat daarbij onderscheid wordt gemaakt tussen verschillende cyberdelicten.

De meest voorkomende technische cyberdelicten zullen hier worden besproken.

Hacking

Hacken is het zich zonder toestemming toegang verschaffen tot een geautomatiseerd werk, zoals een computer, een netwerk of een server waarop websites worden gehost (artikel 80sexies Sr). Hacken wordt in het Wetboek van Strafrecht computervredebreuk genoemd en is een misdrijf dat strafbaar is gesteld in artikel 138ab Sr. Wanneer een hacker vervolgens overgaat tot het stelen (138ab lid 2 Sr) of veranderen, wissen, onbruikbaar of ontoegankelijk maken van gegevens, dan wel het daaraan toevoegen van andere gegevens (350a en 350b Sr), kan er een zwaardere maximumstraf worden opgelegd. Voorbeelden zijn het zonder toestemming toegang verschaffen tot een bedrijfsnetwerk om klantgegevens te verkrijgen, inloggen op een e-mail account om daarmee e-mails te verzenden of toegang verschaffen tot een (sociale media) profielpagina of website om deze te veranderen (CBS, 2020b; Leukfeldt & Yar, 2016; Leukfeldt e.a., 2015; Van ‘t Hoff-de Goede e.a., 2019). Jaarlijks worden veel Nederlanders slachtoffer van hacking, maar de preciese omvang is vooralsnog onduidelijk. Volgens een overzichtstudie van Beerthuizen en collega’s (2020) ligt de omvang van zelfgerapporteerd slachtofferschap van hacking tussen de 1 en 16%. Volgens het CBS (2020b) is in 2019 5,5% van de Nederlanders slachtoffer geweest van hacking. Dit is iets meer dan in 2017 (4,9%), maar minder dan in 2012 (6,0%) (CBS, 2020b). Het aantal ondervonden hacks in 2019 was 8,2 per 100 inwoners (CBS, 2020b). Het inbreken op een website of profielsite kwam daarbij het vaakst voor met 3,2 delicten per 100 inwoners (2,2%) (CBS, 2020b). Uit een verdiepende studie van het CBS bleek dat bij ruim de helft van de slachtoffers (56%) hun socialmedia-account was gehackt en dat bij bijna 3 op de 10 het e-mailaccount werd gehackt (CBS, 2019). In een grootschalig onderzoek onder 1.022 Nederlanders rapporteerden veel respondenten dat het afgelopen jaar hun computer (5%) of account (4%) was gehackt (Van der Grient e.a., 2020). In de studie van Van ’t Hoff-de Goede e.a. (2019; 2021) werd de prevalentie van slachtofferschap van diverse vormen van hacking omschreven, zowel gedurende het afgelopen jaar als daarvoor, zoals het hacken van een e-mailaccount (respectievelijk 0,9% en 3,1%), online-account (0,7% en 2,5%), profielpagina (0,4% en 1,5%) of computer (0,4% en 1,4%).

Malware

Malware is een verzamelnaam voor kwaadaardige software (samentrekking van “malicious software”). Het opzettelijk en wederrechtelijk ter beschikking stellen of verspreiden van gegevens die bestemd zijn om schade aan te richten in een geautomatiseerd werk is strafbaar gesteld in artikel 350a lid 3 Sr. Voorbeelden van malware zijn wormen (die schade aanrichten aan computers), trojan horses (die de overtreder toegang verschaffen tot computer zonder medeweten eigenaar), en spyware (die informatie stuurt van de gebruiker naar een andere partij) (Leukfeldt e.a., 2015). Een vorm van malware die veel (media)aandacht heeft gekregen is ransomware, die de computer blokkeert en waarbij er vervolgens een mededeling verschijnt dat de computer weer vrijgegeven zal worden na het betalen van een bepaald bedrag (Leukfeldt e.a. 2015;

Al-rimy e.a., 2018). Kenmerkend voor ransomware is dat ook back-ups op het systeem versleuteld of verwijderd worden (Brewer, 2016). Ransomware is in staat langere tijd op systemen te verblijven zonder ontdekt te worden, zodat ook back-ups worden versleuteld en herstelopties worden beperkt (Simms, 2016).
Volgens een overzichtstudie van Beerthuizen en collega's (2020) ligt de omvang van zelfgerapporteerd slachtofferschap van malware tussen de 2 (LISS panel) en 62% (Eurobarometer). Het aantal slachtoffers van malware is onder andere moeilijk te bepalen omdat slachtoffers zich er niet bewust van zijn dat ze slachtoffer zijn en de aangiftebereidheid daarnaast beperkt is. De prevalentie van slachtofferschap van malware loopt dan ook uiteen. Onder een steekproef van 1000 Nederlands gaf 16.7% aan slachtoffer te zijn geweest van malware in de afgelopen 12 maanden (Domenie e.a., 2013). Uit een grootschalig onderzoek onder ruim 2400 Nederlanders lag dat percentage wat lager: 7,3% bleek het afgelopen jaar slachtoffer te zijn geworden van malware, waarbij 59% ook (financiële of andere) schade rapporteerde (Van 't Hoff-de Goede e.a., 2019). Bovendien werd 25% van de respondenten eerder al (langer dan een jaar geleden) slachtoffer van malware. Bij nog eens 0,4 en 3,8% van de respondenten waren respectievelijk het afgelopen jaar of langer dan een jaar geleden bestanden ontoegankelijk gemaakt, bijvoorbeeld door ransomware (Van 't Hoff-de Goede e.a., 2019). In een studie van Van der Grient e.a. (2020) onder 1.022 Nederlanders bleek malware een van de meest voorkomende delicten in het afgelopen jaar te zijn geweest; 7% van de respondenten meldde een computer die niet werkte vanwege malware (Van der Grient e.a., 2020). Dat malware een prominent cyberdelict is, blijkt ook uit de bevindingen dat, bij slachtoffers bij wie geld van hun rekening werd geschreven, criminelen in 2,5% van de gevallen via malware aan de gegevens waren gekomen en

dat in 2-2,9% van de gevallen van identiteitsfraude malware de manier was waarop cybercriminelen aan persoonlijke gegevens waren gekomen (CBS, 2019).
Een beperking van de studies over de prevalentie van malware is dat deze gebaseerd zijn op zelfrapportage. Dit vereist namelijk dat het slachtoffer bewust is van het feit dat diens computer is geïnfecteerd. Dat is echter niet altijd het geval. Zo is het mogelijk dat de technologische kennis van het slachtoffer niet toereikend is of dat het slachtoffer geen gebruik maakt van beschermende software die een melding geeft bij een infectie (Holt e.a., 2020). Holt e.a. (2020) hanteerden daarom een meer objectieve meting en vroegen naar de mate waarin computers bepaalde symptomen van malware vertoonden, zoals het verschijnen van een nieuw programma die gebruikers zelf niet hebben geïnstalleerd. In totaal gaf tot 18% van de 5046 respondenten aan dat zij dergelijke symptomen hebben ervaren in de laatste 12 maanden. Dat percentage ligt dus hoger dan op basis van zelfrapportage is te verwachten.

4.2.2. Financiële cyberdelicten

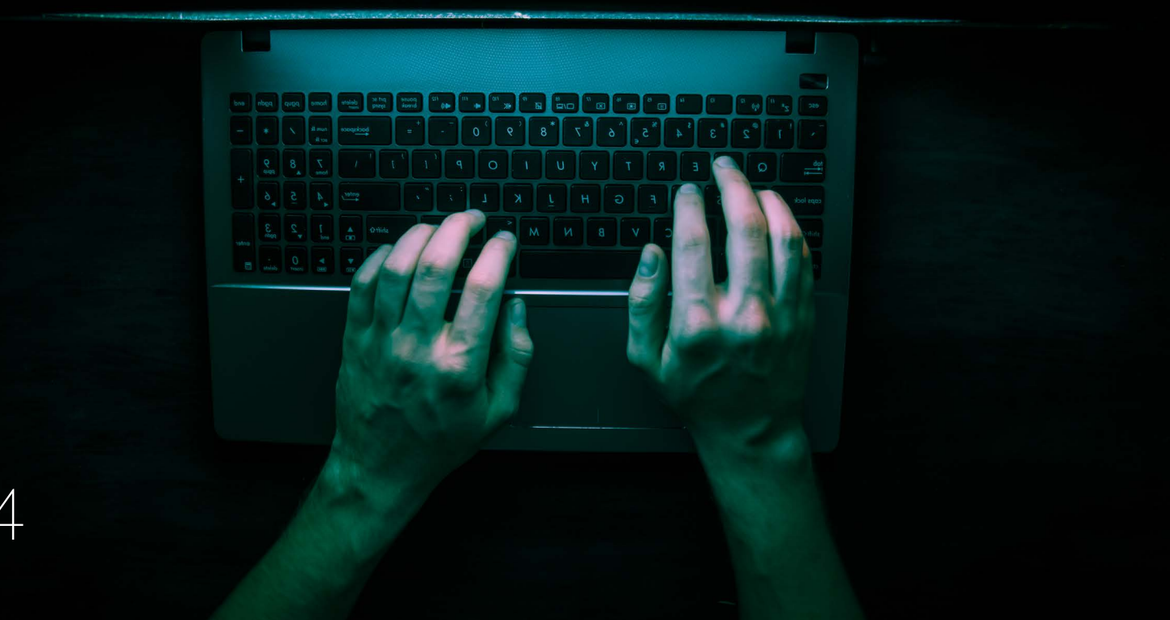
Bij financiële cyberdelicten is het doel van de daders financieel gewin. De meest voorkomende financiële cyberdelicten worden hier besproken.

Phishing

Phishing is een vorm van oplichting waarbij cybercriminelen, bijvoorbeeld via e-mail of websites, inloggegevens proberen te achterhalen om hiermee toegang te krijgen tot accounts, zoals online bankrekeningen (Lastdrager, 2014). Daders maken bijvoorbeeld gebruik van e-mail of WhatsApp om slachtoffers te maken. Hierbij staat "social engineering" centraal, waarbij daders zich voordoen als een voor het slachtoffer bekend persoon of merk (Leukfeldt, 2015; Geng e.a., 2014). Wanneer een phishing-aanval gericht is op specifieke personen of een specifieke groep mensen, wordt ook wel gesproken van spear phishing. Phishing kan strafbaar zijn op grond van artikel 326 Sr (oplichting) of artikel 225 Sr (valsheid in geschrifte).
Phishing is een veel voorkomende vorm van cybercriminaliteit. Het CBS (2019) rapporteerde dat 35% van de internetgebruikers in aanraking was gekomen met phishing maar dat naar schatting "slechts" 1 à 1,5% geld verloren heeft hierdoor. De resultaten van Van 't Hoff-de Goede e.a. (2019; 2021) zijn ongeveer gelijk; 2,9% van de respondenten werd slachtoffer van phishing, waarbij 53% financiële of andere schade opliep door phishing. Een andere reden dat phishing een prominent delict lijkt te zijn, is dat bij slachtoffers van wie geld van de rekening werd gehaald, dit in 30% van de gevallen door phishing kwam (CBS, 2019). Volgens de Nederlandse Vereniging van Banken (2020) hebben bankklanten in 2019 voor bijna 8 miljoen euro aan schaden geleden door phishing, een verdubbeling van het jaar ervoor.

Aankoopfraude

Bij online aankoopfraude (hierna genoemd aankoopfraude) heeft iemand een goed of dienst gekocht en betaald via internet en vervolgens niet gekregen (zie bijvoorbeeld Bloem & Harteveld, 2012; Domenie e.a., 2013). Aankoopfraude is een vorm van oplichting (artikel 326 Sr). Er zou met name worden gefraudeerd met elektronica (mobiele telefoons in het bijzonder) en consumentenartikelen (kleding en accessoires) (Domenie e.a., 2013; CBS, 2018a). Volgens het onderzoek 'Digitale Veiligheid & Criminaliteit' van het CBS (2018a) vindt oplichting meestal plaats via tweedehandsverkoopsites en nepwebshops.
Aankoopfraude is veelvoorkomend. Het percentage slachtoffers schommelt tussen de 2 en 5% (zie Beerthuizen e.a. (2020) voor



een overzicht). In 2019 is volgens het CBS 4,3% van de Nederlanders hiervan slachtoffer geweest, een percentage dat hoger ligt dan in 2017 (2,7%) (CBS, 2020b). De studie van Van 't Hoff-de Goede e.a. (2019; 2021) rapporteerde een lager aantal slachtoffers van online aankoopfraude in het afgelopen jaar (2%) maar vond wel dat 7,8% van de respondenten ooit slachtoffer was geworden van aankoopfraude. In het LISS-panel werd gevonden dat 4% van de respondenten in 2018 slachtoffer was geworden van verkoopfraude (Sipma & Van Leijsen, 2019).

Identiteitsfraude

Bij online identiteitsfraude, strafbaar gesteld in artikel 231b Sr, maakt een crimineel misbruik van persoonlijke informatie[15] van een ander om delicten te plegen, in vele gevallen fraude (Leukfeldt e.a. 2015). Identiteitsfraude kan grote (financiële of andere) schade opleveren voor het slachtoffer. Wanneer criminelen bijvoorbeeld onder hun valse identiteit een creditcard aanvragen of aankopen doen bij webshops met achterafbetaling, kan het slachtoffer van de identiteitsdiefstal opdraaien voor de kosten. Deze kosten worden in een kwart van de gevallen niet vergoed (CBS, 2019), bijvoorbeeld omdat het slachtoffer niet onomstotelijk kan vaststellen dat zij niet zelf deze aankopen heeft gedaan of indien sprake was van grove nalatigheid in het voorkomen van de identiteitsdiefstal (Paulissen & Van Wilsem, 2015). Het gaat gezamenlijk vermoedelijk om enorme bedragen die jaarlijks buitgemaakt worden door middel van online identiteitsfraude (Holt & Turner, 2012). Ook zonder financiële schade kan identiteitsfraude vervelende gevolgen hebben voor slachtoffers, zoals op een zwarte lijst komen te staan van webshops, reputatieschade, of het moeten besteden van veel tijd om de situatie recht te trekken. Hoewel identiteitsfraude behoort tot de meest voorkomende financiële cyberdelicten, lijkt het minder vaak voor te komen dan aankoopfraude en phishing. Het percentage Nederlanders dat het afgelopen jaar slachtofffer werd van een ofmeer vormen van identiteitsfraude loopt in verschillende onderzoeken uiteen van 0,4% tot 4% (CBS, 2020b; Van der Grient e.a., 2020; Van 't Hoff-de Goede e.a., 2019). Het CBS rapporteerde in 2019 0,5%, iets meer dan in 2017 (0,4%) maar lager dan in 2012 (1,5%), een afname die waarschijnlijk veroorzaakt werd door de afname in het cyberdelict skimming (CBS, 2020b). Ook bleek dat in 2018 bij 0,2% van de Nederlanders op hun naam een lening, abonnement, goederen of diensten zijn verkregen (CBS, 2019). In de studie van Van der Grient e.a. (2020) rapporteerde 4% van de ruim 1.000 Nederlandse respondenten dat zij het afgelopen jaar slachtoffer werden van identiteitsdiefstal. In een grootschalige studie onder Nederlandse internetgebruikers waar 0.4% van de respondenten rapporteerde het afgelopen jaar slachtoffer te zijn geworden van online identiteitsdiefstal, meldde 80% schade (Van 't Hoff-de Goede e.a., 2019). Echter, doordat niet alle gevallen van identiteitsfraude bekend zijn bij de slachtoffers ligt het daadwerkelijke aantal slachtoffers vermoedelijk hoger. Het daadwerkelijke aantal slachtoffers van identiteitsfraude blijft ook onduidelijk omdat slachtofferschap met financiële gevolgen niet altijd als zodanig wordt geregistreerd, maar onder andere categorieën valt, zoals vermogensdelicten (CBS, 2019).

15 Het misbruiken van biometrische persoonsgegevens is strafbaar gesteld in art. 231a Sr.

4.2.3. Interpersoonlijke cyberdelicten

Interpersoonlijke cyberdelicten zijn digitale vormen van strafbare gedragsdelicten waarbij de persoonlijke levenssfeer wordt aangetast. Deze delicten kunnen met of zonder seksuele (bij)bedoeling voorkomen. De meest voorkomende interpersoonlijke cyberdelicten zullen hier worden besproken.

Niet-seksuele interpersoonlijke cyberdelicten

De prevalentie van niet-seksuele interpersoonlijke delicten is lastig te bepalen. Volgens het CBS (2019) is 1,4% van de Nederlandse internetgebruikers in 2018 slachtoffer geweest van interpersoonlijke niet- seksuele cyberincidenten. Het gaat daarbij met name om vormen van laster en chantage, gevolgd door stalking en bedreiging met geweld (strafbaar gesteld in artikel 262 Sr (laster), 318 Sr (chantage/afdreiging), 285b Sr (belaging) en 285 Sr (bedreiging). Daar het zelf-rapportage betreft, gaat een groot deel van die incidenten over niet-strafbare feiten, zoals het verspreiden van roddels (0,7%). Wanneer deze niet-strafbare feiten buiten beschouwing wordt gelaten in de cijfers, is naar schatting circa 0,7%-1,2% slachtoffer geweest van niet-seksuele interpersoonlijke cyberdelicten. Onduidelijk is hoeveel van deze slachtoffers meerdere keren slachtoffer werd[16]. Ook op basis van andere bronnen kunnen enkel grove schattingen worden gedaan wat betreft de omvang van slachtofferschap van niet-seksuele interpersoonlijke delicten. Uit het LISS-panel is te herleiden dat 1,8% van de Nederlanders slachtoffer is geweest van online bedreiging in 2018 (zie ook Sipma & van Leijsen, 2019). Het is echter niet te achterhalen of dit enkel betrekking heeft op strafbare vormen van online bedreiging. De helft van de slachtoffers geeft ook aan het voorval niet als ernstig te hebben ervaren. Domenie en collega's (2013) vonden een lager percentage: 0,6% geeft aan slachtoffer te zijn geweest van online bedreiging in het jaar ervoor. Daar bovenop meldde 1% van de slachtoffers slachtoffer te zijn geweest van cyberstalking. Hoewel het in het onderzoek van Domenie e.a. (2013) lijkt te gaan om strafbare feiten, wordt niet gedifferentieerd in seksuele en niet-seksuele incidenten. Ook een meer recente rapportage van het CBS (2020b) maakt geen onderscheid in seksuele en niet- seksuele interpersoonlijke cyberincidenten. Interpersoonlijke delicten komen wel relatief veel voor in politiestatistieken. Het aantal politieregistraties van online bedreiging besloeg circa 3% van het totale aantal registraties in 2016 (Sipma & van Leijsen, 2019).

Seksuele interpersoonlijke cyberdelicten

Sinds de opkomst van internet vinden ook zedendelicten online plaats. Voorbeelden zijn onlinestalkingen intimidatie waarbij de dader seksuele (bij)bedoelingen heeft, bedreiging met seksueel geweld, het zonder toestemming verspreiden van naaktfoto's en –filmpjes (ook wel shame sexting genoemd) of dreigen hiermee (sextortion) (Dodge, 2016; Powell e.a., 2019; Schulz e.a., 2016). Het dreigen met het verspreiden van seksueel beeldmateriaal is strafbaar (chantage/afdreiging, artikel 318 Sr). Het daadwerkelijk zonder toestemming verspreiden van (seksueel) beeldmateriaal is strafbaar gesteld als schending van het portretrecht in artikel 35 van de Auteurswet. Onder bepaalde omstan-

16 Prevalentie van de afzonderlijke niet-seksuele interpersoonlijke delicten: laster zonder roddelen 0.4%, stalking 0.5% en bedreiging met geweld 0,3% (CBS, 2019).

digheden vormt het zonder toestemming online verspreiden van seksueel beeldmateriaal belediging (266 Sr) of smaad (261 Sr). Volgens officiële Nederlandse cijfers werd 0,7% van de internetgebruikers in 2018 slachtoffer van een of meer interpersoonlijke incidenten met een seksuele (bij)bedoeling zoalsstalking, bedreiging met geweld en laster(CBS, 2019). Het gaat hierbij met name om seksueel getinte stalking (0,4%) en laster (0,3%). Met name jongere vrouwen worden slachtoffer: ongeveer drie procent van de 18-25-jarige vrouwen heeft wel eens een cyberincident met een seksuele (bij)bedoeling in de persoonlijke sfeer meegemaakt tegenover 0,8 procent van de mannen in die leeftijd. Onder 12- tot 18-jarigen was dit respectievelijk 2,6 en 0,1% (CBS, 2019). Ongeveer de helft van de slachtoffers van laster en stalking weet wie de dader is, zoals een ex-partner of iemand van school (CBS, 2019). Slechts ongeveer 16% van de slachtoffers doet aangifte bij de politie (CBS, 2019). In werkelijkheid worden echter waarschijnlijk veel meer internetgebruikers slachtoffer van seksuele delicten op internet, zoals uit internationale literatuur is gebleken (zie voor een overzicht: Walker & Sleath, 2017).

Een andere vorm van een seksueel cyberdelict is “sextortion”, oftewel het gebruik van seksueel getint beeldmateriaal als middel om geld of seksuele handelingen af te dwingen bij het slachtoffer.

(Cleiren e.a., 2019). Het gaat hierbij vaak om ex-partners die een hereniging willen afdwingen of wraak willen, of daders die met een enkele verkregen foto meer beeldmateriaal of geld eisen en dreigen anders de foto naar familie en vrienden te sturen (Wolak & Finkelhor, 2016). Cijfers over de prevalentie in Nederland zijn nog niet voorhanden. In Amerika gaf 3% van ondervraagde middelbare scholieren (N=5568) toe gedreigd te hebben met het verspreiden van seksueel beeldmateriaal dat hen was toevertrouwd. Zo’n 5% van de scholieren was slachtoffer geworden van sextortion (Patchin & Hinduja, 2020). Ook uit Australisch onderzoek blijkt dat het dreigen met het verspreiden van seksuele foto’s veelvuldig voorkomt; 5% van de ruim 4000 respondenten uit een nationale survey gaf toe zich hier schuldig aan te hebben gemaakt (Powell e.a., 2019). In totaal had 11,1% van de respondenten zich schuldig gemaakt aan het zonder toestemming maken, verspreiden of dreigen met verspreiden van seksueel beeldmateriaal. Dit hoge percentage daderschap is door onderzoekers gelinkt aan een combinatie van afwijkende seksuele fantasieën en jong, vrijgezel en werkeloos zijn (Babchishin e.a., 2011) en de mogelijkheden die internet meebrengt volgens de routine activiteiten theorie; internet biedt meer toegang tot potentiële slachtoffers en dit maakt het makkelijker voor daders om een geschikt doelwit te vinden (Holt e.a., 2016).

Online zedendelicten kunnen grote impact hebben op de slachtoffers (Leukfeldt e.a., 2018; 2019). Zo zijn er grote emotionele gevolgen, zoals boosheid, eraan blijven denken, slecht slapen en suïcidale gedachten, maar ook bijvoorbeeld financiële gevolgen (Bates, 2017; CBS, 2019; Dodge, 2016; Leukfeldt e.a., 2018). Veel slachtoffers hebben hulpverlening nodig en sommige slachtoffers voelen zich zelfs genoodzaakt te verhuizen (Wolak & Finkelhor, 2016). Emotionele gevolgen worden in veel gevallen versterkt door gebrek aan ondersteuning en begrip in de sociale omgeving en de beperkte mogelijkheden van politie en justitie om daders succesvol aan te pakken (Worsley e.a., 2017; Leukfeldt, Notté & Malsch, 2018; 2019). Daarnaast brengen online zedendelicten nieuwe grote gevolgen met zich mee, zoals dat foto’s die eenmaal online verspreid zijn nooit meer helemaal te achterhalen en verwijderen zijn (Dodge, 2016).

4.2.4. De samenhang tussen verschillende delicten

In het hiervoor genoemde is een overzicht gegeven van de meest voorkomende cyberdelicten anno 2020 in Nederland. In de praktijk is er echter een samenhang tussen deze delicten te zien, zoals ook in de fysieke wereld. Slachtofferschap van online criminaliteit is in sommige gevallen het gevolg van een keten van diverse delicten[17]. Dit zal hier worden toegelicht aan de hand van voorbeelden van de totstandkoming van slachtofferschap van identiteitsfraude.

Om identiteitsfraude te plegen, hebben criminelen persoonlijke of zakelijke gegevens nodig. Voorbeelden zijn naam, adres, telefoonnummer, geboortedatum, accounts, identiteits- en paspoortnummers en bankrekening- of creditcardnummer (Aïmeur & Schofeld, 2011; Paulissen & Van Wilsem, 2015; Gercke, 2007). Criminelen proberen op allerlei manieren aan dergelijke persoonlijke informatie te komen. Ten eerste kunnen criminelen met een gerichte aanval gegevens van een bepaald persoon of bedrijf verzamelen. Een dergelijke gerichte aanval kan bijvoorbeeld plaatsvinden door het stelen van opslagapparaten, infiltreren van een bedrijf (‘insider threat’), het zoeken naar informatie die door bepaalde personen online gedeeld is op bijvoorbeeld sociale media, het gericht hacken van een computer of systeem, of deze infiltreren met malware (Gercke, 2007; Willams, 2016). Een andere online modus operandi is het verzamelen van zoveel mogelijk informatie over zoveel mogelijk personen, waarna deze informatie wordt gekoppeld. Door de opkomst van bijvoorbeeld online winkelen en sociale media wordt er steeds meer dergelijke persoonlijke informatie online opgeslagen. Zo delen werkzoekenden hun cv online, delen sociale media gebruikers veel persoonlijke informatie en vullen talloze online shoppers hun gegevens in op grote hoeveelheden webshops (Christofides & Muise, 2012; Debatin e.a., 2009; Talib e.a., 2010; Aïmeur & Schonfeld, 2011, Sweeney, 2006). Door middel van bijvoorbeeld webscraping kunnen internetcriminelen relatief makkelijk grote hoeveelheden informatie verzamelen. Phishing is ook een veelvoorkomende manier om op grote schaal aan persoonlijke informatie te komen (Williams, 2016; Holt & Turner, 2012). Ook het hacken van bedrijven die grote hoeveelheden klantinformatie bewaren of het gebruik maken van grootschalige datalekken zijn manieren om aan veel persoonlijke informatie te komen. Identiteitsfraude vindt dan ook vaak plaats na het aggregeren van informatie van dergelijke diverse bronnen (Aïmeur & Schonfeld, 2011). Ook kunnen dergelijke grote datasets ook gekocht worden op de zwarte markt en vervolgens gebruikt worden voor het plegen van identiteitsfraude (Caputo e.a., 2014). Ten slotte kan het verzamelen van persoonlijke gegevens stelen van persoonsgegevens ook low- tech gebeuren, door bijvoorbeeld het leeghalen van brievenbussen of het verzamelen van persoonlijke gegevens tijdens een inbraak (Leukfeldt e.a., 2015).

17 Ook wel “crime script” genoemd, zie bijvoorbeeld Dehghanniri en Borrion (2019).

4.3. Welke groepen worden het vaakst slachtoffer van cybercriminaliteit?

Eerdere studies naar slachtofferschap van online criminaliteit hebben geprobeerd een risicoprofiel voor slachtofferschap op te stellen door factoren te identificeren die het risico op slachtofferschap zouden kunnen vergroten. In 4.3.1 zal allereerst een overzicht van deze eerdere studies worden gegeven. Vervolgens zal in 4.3.2 dieper ingegaan worden op twee risicogroepen; jongeren en het mkb (midden- en kleinbedrijf).

4.3.1. Eerder onderzoek naar kenmerken van slachtoffers van cybercriminaliteit

In eerdere studies naar risicofactoren voor slachtofferschap van online criminaliteit staan persoonskenmerken vaak centraal. De meeste studies vinden echter geen duidelijk verband tussen dergelijke kenmerken en het risico op slachtofferschap van cybercriminaliteit (zie ook Van 't Hoff-de Goede e.a., 2019).

Wanneer het slachtofferschap van cybercriminaliteit wordt vergeleken tussen mannen en vrouwen, blijkt dat zij ongeveer even vaak slachtoffer worden (CBS, 2019). Geslacht lijkt niet eenduidig samen te hangen met slachtofferschap van cybercriminaliteit. Aan de ene kant lijken mannen vaker slachtoffer te worden van bepaalde vormen van online criminaliteit, zoals online fraude en hacken (Bossler & Holt, 2010; Van de Weijer & Leukfeldt, 2017). Mannen worden ook vaker slachtoffer van vermogensdelicten dan vrouwen (vijf tegen vier procent) (CBS, 2019).
Aan de andere kant zouden vrouwen juist vaker slachtoffer worden van een malware infectie (Bossler & Holt, 2009; Holt & Bossler, 2013) en phishing (Sheng e.a., 2010) en worden vaker online lastig gevallen (Bossler & Holt, 2010). Studies die zich specifiek richten op identiteitsfraude, spreken elkaar tegen en concluderen dat mannen (Paulissen & Van Wilsem, 2015) of juist vrouwen (Anderson, 2006) vaker slachtoffer worden, of dat er geen verschil op basis van geslacht gevonden is (Domenie e.a., 2013). Voor andere online delicten, zoals hacken, online stalken en online fraude, vonden studies geen verschillen tussen kans op slachtofferschap tussen mannen en vrouwen (Domenie e.a., 2013; Ngo & Paternoster, 2011; Van Wilsem, 2013).
Ook tussen andere persoonskenmerken en slachtofferschap van cybercriminaliteit lijkt geen eenduidig verband te bestaan en een eventueel verband is bovendien zeer afhankelijk van het type cybercriminaliteit waar studies zich op richten. Zo hebben eerdere studies gevonden dat mensen die werken mogelijk vaker slachtoffer worden van malware (Bossler & Holt, 2009) en minder vaak slachtoffer worden van online intimidatie en laster (Ngo & Paternoster, 2011) dan niet-werkenden, maar voor slachtofferschap van hacken is er juist geen verschil tussen de werkenden en niet- werkenden (Domenie e.a., 2013). Ook lijkt zowel het hebben van een hoge als een lage opleiding de kans op slachtofferschap van bepaalde types cybercriminaliteit te verhogen. Lager opgeleiden lijken vaker slachtoffer te worden van hacken (Domenie e.a., 2013) en hoger opgeleiden en personen met hogere inkomens vaker van identiteitsfraude (Paulissen & Van Wilsem, 2015). Bovendien blijkt uit de studie van Domenie en collega's (2013) dat alleenstaanden vaker slachtoffer worden van hacken, maar dit geldt niet voor andere soorten online criminaliteit zoals malware, phishing en cyberstalking (Domenie e.a., 2013).
Onderzoek naar de samenhang tussen leeftijd en slachtofferschap, geeft een duidelijker beeld; veel studies tonen een negatieve correlatie tussen leeftijd en slachtofferschap, wat impliceert dat jongere mensen een grotere kans hebben om slachtoffer te worden en dat deze kans afneemt naarmate de leeftijd toeneemt (Anderson, 2006; Domenie e.a., 2013; Jansen e.a., 2013; Ngo & Paternoster, 2011; Sheng e.a., 2010; Van de Weijer & Leukfeldt, 2017; Van Wilsem, 2013).
Daarnaast is kans op slachtofferschap ook onderzocht in relatie tot de zakelijke wereld. Hierbij komt uit verschillende studies naar voren dat met name het midden- en kleinbedrijf (mkb) een verhoogd risico loopt (zie bijvoorbeeld Alert Online, 2019; Notté e.a., 2019) en in sommige gevallen meer dan eens slachtoffer wordt.
De kenmerken die volgens eerdere studies risico verhogend lijken te zijn voor slachtofferschap van cybercriminaliteit zullen in de volgende paragraaf worden besproken.

4.3.2. Groepen die het vaakst slachtoffer worden van cybercriminaliteit

Op basis van eerder onderzoek zijn er twee risicogroepen naar voren gekomen die een verhoogd risico op slachtofferschap van cybercriminaliteit lijken te hebben: jongeren en het mkb. Deze paragraaf zal op deze groepen ingaan.

Jongeren

De meeste studies waarbij de samenhang tussen leeftijd en online slachtofferschap is onderzocht, wijzen er op dat jongeren vaker slachtoffer worden van online criminaliteit dan oudere personen (Anderson, 2006; Domenie e.a., 2013; Jansen e.a., 2013; Ngo & Paternoster, 2011; Sheng e.a., 2010; Van de Weijer & Leukfeldt, 2017; Van Wilsem, 2013). Dat jongere leeftijdsgroepen vaker slachtoffer worden dan oudere geldt eveneens voor traditionele criminaliteit (CBS, 2020b). Vanaf het 25ste levensjaar is er een lichte daling te zien in slachtofferschap van cybercriminaliteit, en vanaf 55 jaar een grotere

daling (CBS, 2019). Het aandeel 15-24-jarige slachtoffers was in 2019 met 18% ongeveer 2,5 keer zo groot als het aandeel 65-plussers (7%) (CBS, 2020b). Er zijn echter ook studies die geen verband vonden tussen leeftijd en online slachtofferschap voor bijvoorbeeld online identiteitsfraude, oplichting en malware (Bossler & Holt, 2009, 2010; Leukfeldt & Yar, 2016).
Jongvolwassenen van 18 tot 25 jaar hebben het vaakst te maken met interpersoonlijke cyberdelicten, zowel seksueel als niet-seksueel (CBS, 2019; Holt e.a., 2016; Wolak & Finkelhor, 2016), zoals stalking, bedreiging met geweld en laster. Met name jonge vrouwen hebben het vaakst te maken met interpersoonlijke niet-seksuele cyberincidenten, zoals stalken of bedreiging. Ook hebben zij veel vaker dan jongens te maken met cyberincidenten in de persoonlijke sfeer waarbij sprake was van een seksuele (bij) bedoeling (CBS, 2019). Echter geldt dit beeld niet voor alle typen delicten in de studie van het CBS; bij koop- en verkoopfraude en bij hacken zijn ook 25-44-jarigen relatief vaak slachtoffer en bij identiteitsfraude zijn jongeren juist minder vaak slachtoffer dan oudere leeftijdsgroepen (CBS, 2020b).

Midden- en kleinbedrijf (mkb)

Het mkb is ook een belangrijke groep potentiële slachtoffers van cybercrime. Het eerste grootschalige onderzoek naar cybercriminaliteit in het mkb vond dat 28% van de 1203 onderzochte bedrijven slachtoffer is geworden van cybercriminaliteit, voornamelijk van malware, aankoopfraude, phishing en hacken (Veenstra e.a., 2015). Het CBS (2018b) rapporteerde dat in 2016 slachtofferschap onder bedrijven hoog was. Van de bedrijven met 2 tot 10 werknemers ervaarde 26% een ICT- veiligheidsincident. Bij bedrijven met meer dan 10 werknemers was dit zelfs 50%. Slechts respectievelijk 6 en 9% van deze bedrijven deed melding van het incident. In 2019 is een nulmeting uitgevoerd om te onderzoeken hoeveel mkb-bedrijven slachtoffer geworden zijn van cybercrime (Notté e.a., 2019). De grootste groep slachtoffers geeft aan slachtoffer te zijn geworden van cybercriminaliteit (criminaliteit gericht op ICT; 17,9%), waarvan malware (30,9%) en ransomware (17,2%) de meest genoemde delicten zijn. De kleinste groep geeft aan slachtoffer te zijn geworden van gedigitaliseerde criminaliteit (traditionele criminaliteit op internet; 8,8%). Deze groep bestaat met name uit slachtoffers van phishing (9,9%). Ook werden er enkele bedrijven slachtoffer van beide soorten cybercrime (Notté e.a., 2019). Mkb-bedrijven met minder dan tien medewerkers leken hierbij minder vaak slachtoffer van cybercrime te worden dan mkb-bedrijven met meer personeel. Omzet en sector leken niet samen te hangen met slachtofferschap. Het hebben van IoT (Internet of Things), niet werken met interne autorisaties op het bedrijfsnetwerk en het toegang verlenen van externen op het bedrijfsnetwerk hangen samen met een verhoogde kans op slachtofferschap van cybercrime (Notté e.a., 2019).
Recente andere verkennende onderzoeken vonden eveneens dat mkb'ers relatief vaak slachtoffer worden van cybercriminaliteit. Zo vonden Misana-ter Huurne en collega's (2020) dat 65% van de door hun ondervraagde mkb'ers ooit slachtoffer is geworden; sommigen meer dan eens. De helft hiervan heeft schade ondervonden. Ook bleek dat 8% in het afgelopen jaar slachtoffer was geworden, waarbij hacking het meest genoemde delict is (Misana-ter Huurne e.a., 2020). Een ander verkennend onderzoek in de Nederlandse metaalsector vond dat zeven van de tien mkb-bedrijven slachtoffer was geworden van een of meerdere types cybercriminaliteit, waarbij vier bedrijven malware op hun systeem hadden gehad (Notté, Van 't Hoff-de Goede & Leukfeldt, 2019). In een onderzoek naar de cyberweerbaarheid onder 56 Haagse winkeliers, bleek bijna de helft (48%) van de retailers slachtoffer te zijn geweest van cybercrime in het voorafgaande jaar - het vaakst van phishing - waarbij zeven bedrijven (12%) ook schade hiervan hadden ondervonden (Van der Kleij, De Bruin, Van 't Hoff-de Goede & Leukfeldt, 2019). Ook Alert Online (2019) heeft onderzoek gedaan naar slachtofferschap van cybercriminaliteit. Zo geeft circa 32% van het mkb aan wel eens te maken te krijgen met phishing, waarmee dit vaker voorkomt dan andere cyberdelicten. Ongeveer een derde daarvan heeft ook wel eens op een phishinglink geklikt. Mkb'ers schatten het risico om slachtoffer te worden bovendien relatief laag in vergeleken met andere doelgroepen (Alert Online, 2019; Notté e.a., 2019).
Bovengenoemde resultaten uit Nederlandse studies zijn in lijn met bevindingen uit het buitenland. Ook in andere landen zijn de cijfers hoog: een survey van streamingsdienst Beaming onder het mkb in het Verenigd Koninkrijk laat zien dat circa 60% van de bedrijven slachtofferschap van cybercriminaliteit rapporteert. In de meeste gevallen ging het hierbij om phishing en malware (Beaming, 2018).

4.4. Deelconclusie inzichten uit de literatuur

Verschillende nationale en internationale wetenschappelijke studies en grootschalige bevolkingsonderzoeken uit Nederland zijn geraadpleegd om uitspraken te doen over slachtofferschap van cybercriminaliteit. Dit literatuuronderzoek wijst uit dat het aantal daadwerkelijke slachtoffers van cybercriminaliteit lastig te bepalen is. Zo doen slachtoffers niet in alle gevallen aangifte of weten ze niet dat ze slachtoffer zijn geweest, waardoor cijfers onvolledig zijn. Ook worden gemelde delicten niet altijd op de juiste manier geregistreerd of gemeten. Over het algemeen ontstaat uit het literatuuronderzoek wel het beeld dat het totale aantal slachtoffers van cybercriminaliteit in Nederland op meer dan tien procent ligt en dit aantal de laatste jaren is toegenomen.
Op basis van eerder onderzoek komen er twee risicogroepen naar voren die vaker slachtoffer lijken te worden van cybercriminaliteit dan andere doelgroepen: jongeren en het mkb. Jongeren van 18 tot 25 jaar lijken vaker slachtoffer te worden dan oudere personen, zoals ook het geval bij traditionele criminaliteit. Jongeren krijgen met name te maken met interpersoonlijke delicten, zowel seksueel als niet-seksueel, waarbij jonge vrouwen in het bijzonder worden genoemd als slachtoffer. Naast jongeren, blijkt ook uit nationale en internationale studies dat het aantal mkb'ers dat slachtoffer wordt van cybercriminaliteit relatief hoog is vergeleken met andere groepen. De meest genoemde delicten bij de doelgroep mkb'ers zijn malware, hacking en phishing. In tegenstelling tot jongeren, lijkt bij de slachtoffergroep mkb'ers dus voornamelijk technische cybercriminaliteit voor te komen.
Binnen de drie categorieën van cybercriminaliteit (technische delicten, financiële delicten en interpersoonlijke delicten) komt een aantal delicten naar voren die het mees-

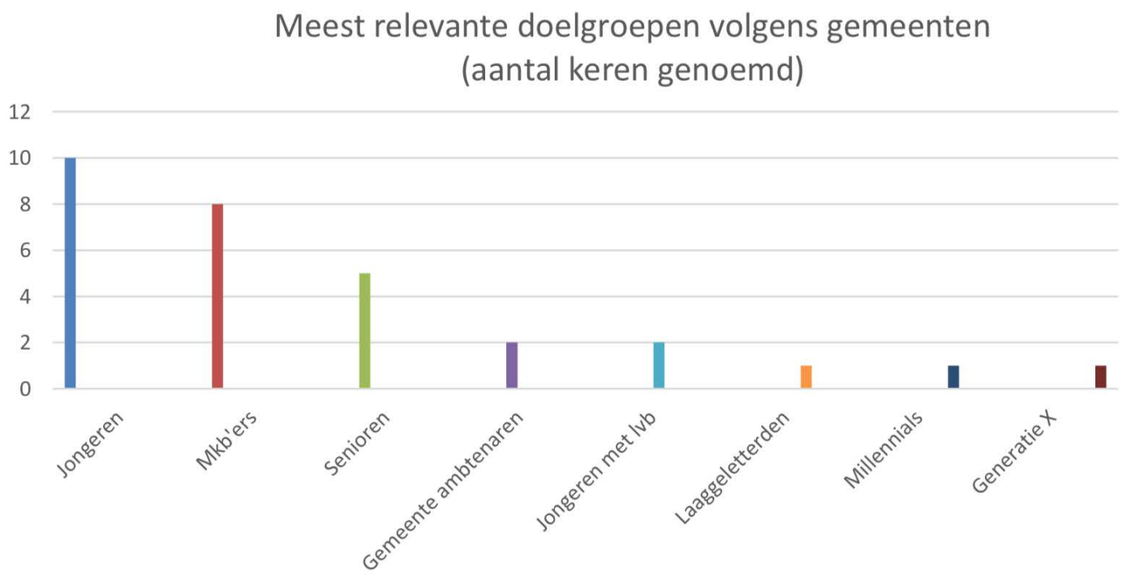
“ Volgens de literatuur zijn jongeren en mkb’ers de belangrijkste risicogroepen voor slachtofferschap van cybercriminaliteit.”

te voorkomen. Deze delicten treden niet altijd afzonderlijk van elkaar op: phishing of hacking, bijvoorbeeld, gaan vaak
Volgens de literatuur zijn jongeren en mk-b’ers de belangrijkste risicogroepen voor slachtofferschap van cybercriminaliteit. vooraf aan het plegen van identiteitsfraude. Slachtofferschap is dus vaak een gevolg van een serie aan delicten. Binnen de categorie technische cyberdelicten lijken met name hacking en malware vaak voor te komen, waarbij de percentages slachtoffers tussen studies sterk uiteenlopen. Bij deze delicten speelt in het bijzonder een rol dat slachtoffers niet altijd bewust zijn van het feit dat ze slachtoffer zijn geweest, waardoor objectieve metingen een nog groter percentage vinden dan studies gebaseerd op zelfrapportage. Wat betreft financiële cyberdelicten worden vooral online aankoopfraude, phishing en identiteitsfraude genoemd. In het geval van interpersoonlijke cyberdelicten lijken seksueel getinte stalking en niet-seksuele interpersoonlijke delicten zoals online bedreiging in Nederland het vaakst voor te komen.

“ Volgens de literatuur zijn de meest voorkomende cyberdelicten per categorie: Technische cyberdelicten: hacking en malware (inclusief ransomware) Financiële cyberdelicten: phishing, online aankoopfraude en identiteits-fraude Interpersoonlijke cyberdelicten: seksueel getinte stalking en online bedreiging “

5. INZICHTEN UIT DE PRAKTIJK

In dit hoofdstuk worden de deelvragen die centraal staan in dit rapport beantwoord op basis van inzichten uit de praktijk. In 5.1 wordt ingezoomd op de meest relevante doelgroepen (5.1.1) en typen cybercriminaliteit (5.1.2) volgens de vertegenwoordigers van de deelnemende gemeenten en wordt beschreven op welke manieren respondenten dit onderbouwen (5.1.3). Vervolgens worden in 5.2, op basis van de resultaten van de interviews met deskundigen uit het werkveld van cybercriminaliteit aanvullende inzichten beschreven. Hierbij zal eerst worden beschreven wat, volgens deze experts, de meest voorkomende slachtoffergroepen (5.2.1) en typen cybercriminaliteit (5.2.2) zijn. Vervolgens wordt besproken welke groepen en typen delicten deze experts hebben aangemerkt als meest relevant om de cyberweerbaarheid het eerst voor te verhogen (5.2.3). Tot slot zijn op basis van de eerste twee interviewrondes deze inzichten getoetst aan de kennis en ervaring van praktijkpartners die dagelijks met de geselecteerde doelgroepen werken (5.3). Tot slot zal in 5.4 een deelconclusie worden getrokken over inzichten die zijn opgedaan in uit de praktijk.



Figuur 1. Meest relevante doelgroepen volgens gemeenten (N=12)

5.1. Gemeenten

5.1.1. Meest relevante doelgroepen volgens gemeenten

Uit de interviews met vertegenwoordigers van de gemeenten[18] (N=12) komt een aantal doelgroepen naar voren waarvoor het volgens de gemeenten het meest noodzakelijk is om de cyberweerbaarheid van te vergroten. Dit betekent dus niet (per se) dat de gemeenten nu zelf al actief interventies uitvoeren gericht op deze doelgroepen, maar dat ze dit zien als prominente doelgroepen. In Figuur 1 is hiervan een overzicht te vinden. Hieruit blijkt, dat jongeren (tien keer genoemd), mkb'ers (acht keer genoemd) en ouderen/senioren (vijf keer genoemd) volgens de respondenten de meest relevante doelgroepen zijn om de cyberweerbaarheid van te verhogen.
Tevens is gevraagd waarom de respondenten elke doelgroep hebben aangedragen als meest noodzakelijk. Sommige gemeenten hebben meerdere doelgroepen genoemd.
In Tabel 2 staan per doelgroep de meest genoemde toelichtingen die respondenten hebben gegeven bij hun keuze.

Tabel 2. Meest genoemde toelichtingen voor keuze van doelgroepen door gemeenten (N=12)

Doelgroep	Toelichting
Jongeren/jeugd	Jongeren zijn kwetsbaar: groeien op in de digitale wereld en zijn zich niet bewust van gevaren Delicten hebben een grote impact op het leven van jongeren Omvang cybercriminaliteit bij de doelgroep is groot
Mkb-ondernemers	Delicten hebben een grote impact: ondernemers hebben een groot financieel belang Omvang cybercriminaliteit bij de doelgroep is groot
ouderen/senioren	Ouderen zijn kwetsbaar: niet digitaal geschoold en dus onbekend met de digitale wereld
gemeenteambtenaren	De eerste stap is dat gemeenten zelf goed beveiligd zijn Gemeenten beschikking over veel gevoelige data
jongeren met lvb	Extra kwetsbaar vanwege moeite met inschatten gevaren en consequenties van daden
Laaggeletterden	Laaggeletterden zijn digitaal minder vaardig en dus kwetsbaar
Millennials	Omvang cybercriminaliteit bij de doelgroep is groot
Generatie X	Omvang cybercriminaliteit bij de doelgroep is groot

18 Respondenten zijn óf in dienst als ambtenaar openbare orde en veiligheid óf vervullen een functie die specifiek gericht is op cybercriminaliteit of cyberweerbaarheid voor de betreffende gemeente.

De doelgroep die het meest genoemd is, zijn jongeren: tien van de twaalf gemeenten zien jongeren als (één van de) meest relevante, kwetsbare doelgroep om de cyberweerbaarheid van te verhogen. Veelgenoemde redenen hierbij zijn dat jongeren opgroeien in een digitale wereld, relatief veel tijd online spenderen, en online gevaren niet altijd zien. Dat laatste is volgens respondenten voor jongeren met een licht verstandelijke beperking (lvb) in hogere mate het geval. De belangrijkste afweging lijkt echter dat cyberdelicten volgens respondenten een grote impact hebben op het leven van jongeren, met name in het geval van interpersoonlijke delicten, zoals shame sexting / sextortion en cyberpesten (zie ook 5.1.2). De onderbouwing van de uitspraken over risicogroepen wordt nader besproken in paragraaf 5.1.3.

"Ik denk sowieso jongeren, want die groeien op binnen een compleet digitale wereld. Dus als we daar ouderwets mee omgaan en zeggen: "Nee, het bestaat allemaal niet." Dan ben je nu al te laat." - (GEM12)

De definiëring van de doelgroep 'jongeren' verschilt per gemeente. Zo richt GEM11 zich op jongeren onder de 12 jaar, GEM3 hanteert een leeftijd van 8 tot 30 jaar, GEM10 noemt jongeren tot 23 jaar en GEM12 heeft het over jongeren tot 18 jaar. Naast jongeren noemen twee gemeentes ook "ouders" als doelgroep, maar dan als een manier om de jongeren te benaderen/beïnvloeden.
De tweede prominent geachte risicogroep is het midden- en kleinbedrijf (mkb), genoemd door acht gemeenten. Hierin worden in de basis geen subgroepen onderscheiden (hoewel soms in het algemeen van "ondernemers" wordt gesproken). De reden om mkb'ers als doelgroep aan te merken, ligt vooral in de mogelijke financiële schade voor deze bedrijven en de risico's die dit met zich meebrengt voor de ondernemer. Daarnaast worden mkb'ers gezien als aantrekkelijke doelwitten waar voor criminelen veel gewin te behalen is. De impact van delicten lijkt dus ook hier een belangrijke afweging, zoals ook het geval bij jongeren.

"Ik denk dat het voor ondernemers heel belangrijk is, omdat zij voor hun werk en inkomsten heel afhankelijk zijn en daardoor heel kwetsbaar. Zij werken vaak met veel data, waarbij data de sleutel is, het belangrijkste in hun bedrijf. Als daar iets mee gebeurt, dan heeft dat meteen enorme consequenties." - (GEM1)

Een gemeente maakt nog wel de opmerking dat in de context van de problematiek mkb'ers zich beter organiseren en luider laten horen dan bv. jongeren, en zo als slachtoffer wellicht meer opvallen.
Volgens vijf gemeenten vormen ouderen/senioren bovendien een relevante en kwetsbare doelgroep. Hierbij worden geen specifieke subgroepen aangemerkt. De belangrijkste redenen voor het aandragen van ouderen/senioren als noodzakelijke doelgroep zijn de veronderstelde lage weerbaarheid - gevoed door beperkte digitale vaardigheden en kennis van cybercriminaliteit – in combinatie met het soms (te) goed van vertrouwen zijn.

"Bij ouderen (..) wat je met babbeltrucs en woninginbraken doet, dat moet je nu op dit vlak ook gaan doen." - (GEM12)

Andere specifieke doelgroepen die worden benoemd door respondenten zijn gemeenteambtenaren, laaggeletterden, millennials (grofweg mensen tussen de 20 en 40 jaar) en Generatie X (grofweg mensen tussen de 40 en 60 jaar). Millennials en Generatie X worden volgens officiële cijfers (politieregistraties) vaak slachtoffer van cybercriminaliteit en zouden dus een focus moeten zijn van gemeenten, aldus één gemeente. Gemeenteambtenaren zelf worden ook genoemd, omdat gemeenten veel persoonsgegevens verzamelen en over sensitieve data beschikken, met name ook door de digitalisering van gemeenten. Laaggeletterden worden genoemd, omdat zij minder digitaal vaardig zouden zijn, hoewel dit op persoonlijke inschattingen berust. Eén gemeente stelt bovendien dat eigenlijk de hele bevolking doelgroep is, aangezien iedereen slachtoffer kan worden.

"Eigenlijk heb je de hele bevolking als doelgroep, zou je kunnen zeggen. En allemaal op verschillende punten. Dat is niet echt behapbaar. Vandaar dat je keuzes maakt. Daar moeten we ook een kanteling in de samenleving uiteindelijk in maken. Dat de hele samenleving zich daar ergens steeds bewuster van gaat worden." - (GEM12)

5.1.2. Meest relevante typen cyberdelicten volgens gemeenten

Uit de interviews met gemeenteambtenaren komen verschillende typen cybercriminaliteit naar voren waarvoor het vergroten van de cyberweerbaarheid het meest noodzakelijk wordt geacht. Tabel 3 bevat een overzicht van die typen cybercriminaliteit. Ook hierbij hebben sommige gemeenten meerdere delicten aangemerkt.

Tabel 3. Meest relevante cyberdelicten om de cyberweerbaarheid tegen te vergroten volgens gemeenten (N=12)

Typen cybercriminaliteit	Aantal keren genoemd (i.c.m. doelgroep)
Shame sexting/ sextortion	7 keer in combinatie met de doelgroep jongeren
Phishing	7 keer in combinatie met de doelgroep jongeren
Aankoop- en verkoopfraude	3 keer, waarvan in combinatie met doelgroepen: jongeren (1), mkb (1) en iedereen (1)
Malware / ransomware	3 keer in combinatie met de doelgroep mkb
DDos-aanval	3 keer in combinatie met de doelgroep mkb
Whatsapp-fraude / Vriend- in- noodfraude	3 keer, waarvan in combinatie met doelgroepen: iedereen (2) en ouderen (1)
Identiteitsfraude	2 keer in combinatie met de doelgroep jongeren
Cyberpesten en online intimidatie	1 keer in combinatie met de doelgroep jongeren
Geldezelen[19]	1 keer in combinatie met de doelgroep jongeren
Hacken	1 keer in combinatie met de doelgroep mkb
Helpdeskfraude	Niet genoemd

Shame sexting / sextortion onder jongeren wordt door zeven van de twaalf gemeenten aangedragen als meest noodzakelijke type cybercriminaliteit om interventies op te richten. Met name de impact op slachtoffers is hierbij van belang. Zo maakt de aard van het internet dat het bereik van seksueel getint materiaal veel groter is geworden en foto’s voor altijd online kunnen blijven (GEM3). Het delict brengt dan ook grote emotionele schade toe, aldus GEM8.

“Ik denk dat dat sexting, dat kan echt heel lelijk uit de hand lopen, omdat als er pikante foto’s worden gedeeld - krijg die maar eens offline.” - (GEM3)

Het is volgens verschillende gemeenten ook lastig om zicht te krijgen op het delict. Zo wordt er weinig aangifte gedaan en komt het delict dus niet terug in de politiecijfers; jongeren vinden het wellicht moeilijk om erover te praten, aldus GEM9. Gemeenten horen op basis van signalen uit de omgeving

dat de omvang van het delict groot is. Zo haalt een respondent het voorbeeld aan van een middelbare school die twee bij de school bekende sexting incidenten per jaar heeft. Soms is er volgens GEM9 ook sprake van jongeren die elkaars social media-accounts hacken en op die manier seksueel getint materiaal verspreiden.
“Bij jongeren is de impact van sexting bijvoorbeeld heel groot. Het komt veel voor, hoeveel weten we niet precies. Onlangs had een collega ook een kleine studie ervan gemaakt, ja daar schrik ik wel van. Dan denk ik echt: knetters, dat dat al zo veel gebruikt wordt, gebeurt en zo gewoon al is geworden.” - (GEM3)

Phishing wordt door vier gemeenten genoemd. Opvallend hierbij is dat er geen sterke koppeling lijkt te zijn met een doelgroep: iedereen kan hiervan slachtoffer worden. Wel worden expliciet de phishingvormen *whaling* of *CEO-fraude*[20] genoemd die specifiek op het mkb zijn gericht, en een hoge opbrengst voor daders kunnen opleveren, met daaraan gekoppeld veel schade voor de slachtoffers.
Vier typen delicten worden driemaal genoemd door de gemeenten. DDos-aanvallen en malware/ransomware zouden sterk op het mkb gericht zijn, en leggen bijvoorbeeld bedrijfsprocessen stil met alle gevolgen

19 Een geldezel (of money mule) is een katvanger die zijn of haar bankrekening laat misbruiken voor criminele activiteiten. Hij is in feite een geldkoerier die, bewust of onbewust, meewerkt aan het witwassen van crimineel geld of het doosluizen van gestolen geld. Een crimineel (of criminele organisatie) maakt gebruik van de geldezel om anoniem indirect geld op te nemen van een bankrekening waarover de crimineel onrechtmatig de beschikking heeft om geld over te maken, of hij licht bijvoorbeeld iemand op door iets te verkopen maar niet te leveren, en daarbij de koper geld over te laten maken op de rekening van de geldezel. De geldezel ontvangt hiervoor doorgaans een geldbedrag. De geldezel is daarmee aansprakelijk voor het doorgesluisde geld, bijvoorbeeld als onverschuldigde betaling. Als hij had moeten begrijpen dat hij een crimineel hielp is hij ook strafbaar. Een naïeve geldezel is ook te beschouwen als slachtoffer.

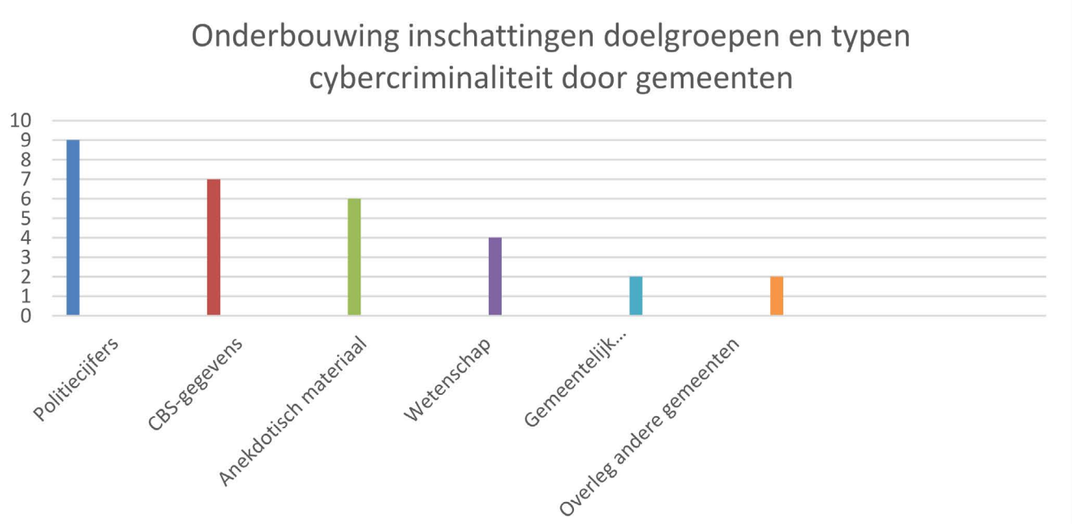
20 CEO-fraude of whaling is een vorm van fraude of oplichting waarbij er geprobeerd wordt om mensen geld te laten overmaken naar de bankrekening van de oplichter door zich voor te doen als een CEO of andere hooggeplaatste functie van een bedrijf. CEO-fraude is een vorm van factuurfraude.

van dien. Van Whatsappfraude kan volgens GEM5 iedereen slachtoffer worden, zoals terug te zien in trendrapportages van de politie. Hoewel niet iedereen daadwerkelijk slachtoffer wordt, worden wel veel mensen benaderd door fraudeurs, aldus GEM9. Omdat accurate cijfers ontbreken, is het lastig te bepalen of sommige doelgroepen vaker slachtoffer worden van dit delict. GEM9 ziet in politiecijfers dat het delict vooral onder ouderen voorkomt. Aan- en verkoopfraude kan iedereen treffen die bv. via Marktplaats handelt, maar ook de mkb'er wiens producten niet betaald worden. De omvang van dit delict kan sterk variëren.

Ten slotte wordt een aantal delicten een keer genoemd door gemeenten. Dit betreffen identiteitsfraude, cyberpesten en online intimdatie, geldezelen en hacken. Ook hierbij wordt meestal gerefereerd naar de impact en omvang van het delict. Tevens stelt één gemeente dat het van belang is dat gemeenten zich richten op nieuwe delicten in het algemeen, omdat gemeenten daar makkelijk risicocommunicatie op kunnen zetten en er in de toekomst constant nieuwe delicten zullen komen. Wel zijn volgens deze respondent actuele, regionale politiecijfers nodig om zicht te krijgen op dergelijke trends.

5.1.3 Onderbouwing

Ter verdieping is aan respondenten gevraagd waar zij inschattingen over slachtofferschap op baseren. Hieruit blijkt, dat alle ondervraagde gemeenten gebruik maken van cijfers van de politie en/of het CBS. Een overzicht van die bronnen is te vinden in Figuur 2. Deze bronnen kunnen over het algemeen beschouwd worden als de basis voor het gemeentelijke interventiebeleid (voor zover aanwezig) op het gebied van cybercriminaliteit. Zo geeft GEM10 aan cijfers te gebruiken ter onderbouwing van de aanpak van cybercriminaliteit en om politieke aandacht te vragen.



Figuur 2. Overzicht onderbouwing doelgroepen en typen cybercriminaliteit door gemeenten (N=12)

Negen van de twaalf gemeenten geven aan beschikking te hebben over politiecijfers of trendanalyses van de politie. Dit betreft bijvoorbeeld aangiftedata van het LMIO, kwartaalrapportages van de eenheden of informatie verkregen van digitale wijkagenten. Echter stellen de meesten van die gemeenten dat politiecijfers slechts beperkt of niet bruikbaar zijn. Zo zijn de cijfers te breed: de politie registreert in principe enkel algemene categorieën van cybercriminaliteit, zoals horizontale fraude[21]. Bovendien zou de aangiftebereidheid onder burgers laag zijn, waardoor cijfers over slachtofferschap in de gemeente niet representatief zijn voor de werkelijkheid. Hierdoor geven volgens een respondent politiegegevens weinig inzicht in specifieke doelgroepen en de typen cybercriminaliteit waarvan zij slachtoffer van worden. Een andere gemeente geeft aan dat zij regionale cijfers bruikbaarder vinden om trends te identificeren, omdat dit volgens hen inzichten op grotere schaal (gemeente overschrijdend) geeft.

"Ik hou van cijfers, tegelijkertijd weet ik ook dat ze maar een deel van de werkelijkheid laten zien. Het helpt gewoon om toch een beetje te schetsen hoe iets is." - GEM3.

Naast politiecijfers, geven zeven gemeenten aan gebruik te maken van landelijke of gemeentelijke (slachtoffer)cijfers van het CBS. Volgens GEM10 zijn deze cijfers betrouwbaarder dan die van de politie, vanwege de lage aangiftebereidheid onder burgers. Twee gemeenten geven echter aan dat ook de cijfers van het CBS te globaal zijn om richting te geven aan interventies. Andere genoemde bronnen voor informatie over slachtofferschap zijn wetenschappelijke studies, gemeentelijk bevolkingsonderzoek en overleg met andere gemeenten.

Officiële cijfers over slachtofferschap van cybercriminaliteit lijken dus beperkt bruikbaar[22] voor gemeenten, omdat ze een onjuist beeld schetsen van de werkelijkheid en weinig handelingsperspectief bieden. De helft van de gemeenten geeft dan ook aan inschattingen over slachtofferschap te baseren op anekdotisch materiaal, zoals gevoel, 'gezond verstand' of signalen en verhalen uit de omgeving.

"Dit zijn allemaal voor de hand liggende doelgroepen, toch wel de kwetsbare mensen die wij zien. Maar dat is eigenlijk nergens op gestoeld, puur op gezond verstand." - (GEM1)

"Dat is eigenlijk moeilijk te zeggen vanwege dat grote dark number, maar dat is meer de geluiden die je hoort in de omgeving en als het gesprek er over gaat en de dingen die je erover leest." - GEM5

Bij de prioritering van relevante doelgroepen valt op dat keuzes niet altijd (puur) op basis van cijfers worden gemaakt. Er wordt soms een afweging gemaakt om, naast prevalentie (het voorkomen van een vorm van cybercri-

21 Horizontale fraude betreft alle fraude die is gericht tegen burgers, bedrijven en financiële instellingen en niet tegen de overheid.

22 De helft van de ondervraagde gemeenten (6) benoemt het gebrekkige zicht op het fenomeen cybercriminaliteit ook als belemmering ter bevordering van de cyberweerbaarheid van burgers, wat vaak samenhangt met een beperkte capaciteit en expertise (GEM1, GEM2, GEM5, GEM6, GEM11 en GEM12). Genoemde oplossingsrichtingen hiervoor zijn onder meer landelijke monitoring van cybercriminaliteit en coördinatie vanuit de overheid en meer ondersteuning vanuit partners of andere (grote) gemeenten. De behoefte aan ondersteuning wordt breed erkend onder de respondenten.

minaliteit), vooral ook de omvang en duur van de impact die cybercriminaliteit kan veroorzaken op (het leven van) een doelgroep als uitgangspunt te nemen voor de prioritering van doelgroepen. Hiermee wordt soms gekozen voor (in aantallen) minder voorkomende vormen van cybercriminaliteit, maar die des te meer of grotere (langdurige) negatieve gevolgen kunnen hebben voor de slachtoffers.

Volgens de gemeenten is het verhogen van de cyberweerbaarheid per doelgroep vooral van belang bij de volgende typen cyberdelicten:

1) Jongeren: Shame sexting / sextortion,
2) Ouderen: Vriend-in-nood-fraude en
3) Mkb'ers: Malware (ransomware) en DDos-aanval
Daarnaast komt naar voren dat phishing een belangrijk cyberdelict is, waarbij van iedereen de cyberweerbaarheid verhoogd moet worden.

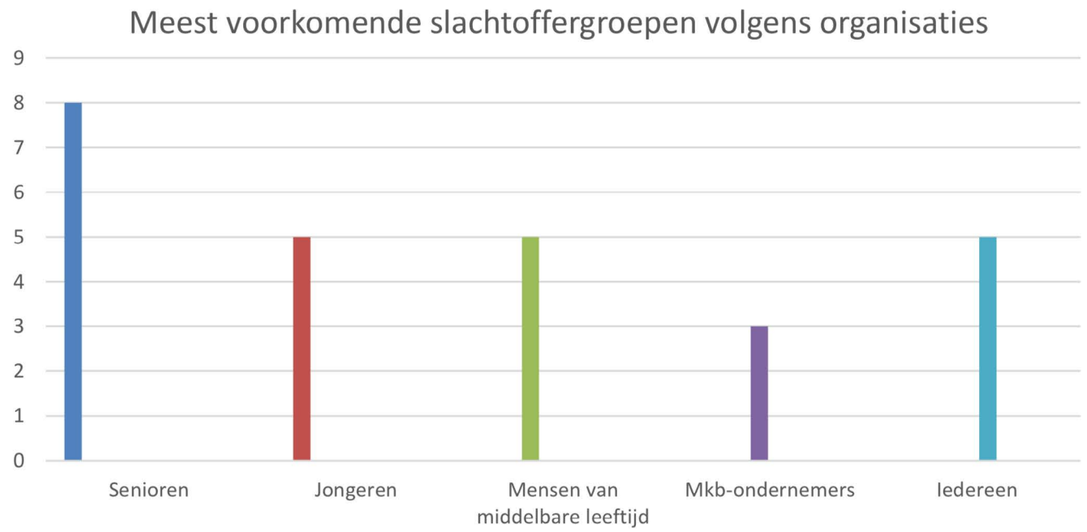
5.2. Experts

In deze paragraaf zal worden besproken welke doelgroepen volgens de experts het vaakst slachtoffer worden van cybercriminaliteit (5.2.1). Vervolgens zal worden beschreven welke typen cybercrime het meeste voorkomen volgens deze respondenten (5.2.2). Vervolgens zal worden besproken voor welke doelgroepen en typen cybercrime, volgens de experts, interventies om de slachtofferschap terug te dringen het meest noodzakelijk zijn (5.2.3).

5.2.1 Meest voorkomende doelgroepen volgens experts

Uit de interviews met experts op het gebied van slachtoffergroepen komen een aantal doelgroepen naar voren die het meeste slachtoffer worden van cybercriminaliteit. In Figuur 3 is hiervan een overzicht te vinden. Hieruit blijkt, dat ouderen (N=8), jongeren (N=5), mensen van middelbare leeftijd (N=5) en mkb'ers (N=3) volgens de respondenten de meest voorkomende slachtoffergroepen zijn. Ook wordt 'iedereen' aangehaald als doelgroep (N=5). In Tabel 4 staat bovendien beschreven waarom volgens de respondenten de genoemde doelgroepen slachtoffer worden van cybercriminaliteit .
Opvallend is dat experts moeite lijken te hebben met het aanwijzen van specifieke slachtoffergroepen; volgens de meeste respondenten kan iedereen slachtoffer worden van cybercriminaliteit. Zo wordt ook een aantal factoren genoemd die in het algemeen een rol spelen bij slachtofferschap, zoals beperkte computervaardigheden en een gebrek aan kennis (EXP1 en EXP13). De politie herkent dat aangevers vaak geen idee hebben wat hen precies is overkomen. Ook wordt de rol van daderschap aangehaald: daders maken misbruik van bestaande technieken en de onwetendheid die daar rondom heerst. Dat is niet gebonden aan een specifieke doelgroep.
"En wat je wel ziet is dat bepaalde vormen van cybercriminaliteit meer voorkomen in een doelgroep dan andere. Maar in de volledige breedte kan iedereen slachtoffer worden van cybercrime." - (EXP1)

"Denk aan Marktplaats Gelijk Oversteken: het systeem wat Marktplaats veiliger zou moeten maken. Marktplaats implementeert dat, en vervolgens zie je dat er een enorme onwetendheid is over: wat is dat nou precies. En van die onwetendheid wordt gebruik gemaakt..." - (EXP1)
Toch wordt er door de experts ook duidelijk



Figuur 3. Meest voorkomende slachtoffergroepen volgens experts (N=9)

gerefereerd aan vier specifieke doelgroepen: ouderen, jongeren, mensen van middelbare leeftijd en mkb'ers. Deze doelgroepen worden genoemd in combinatie met specifieke delicten.
Ouderen worden het vaakst genoemd door de respondenten, maar het verschilt bij welke leeftijd die groep begint: zo komt 50, 60 en 70 jaar terug in de interviews als ondergrens (EXP4, EXP9 en EXP16). Dit is gekoppeld aan de registratiemethode van de organisaties en lijkt ook afhankelijk van het type delict. Zo zijn volgens EXP4 vooral zeventigplussers doelwit van spoofing. Datingfraude zou vooral mensen vanaf ongeveer 50 jaar treffen; met name vrouwen die gescheiden zijn of waarvan de partner overleden is (EXP15). Ouderen zouden kwetsbaar zijn omdat zij relatief veel geld bezitten, vanwege beperkte digitale vaardigheden en goedgelovigheid (EXP1, EXP3, EXP4, EXP6, EXP7, EXP9 en EXP16). Daarom zijn ouderen specifiek doelwit van cybercriminaliteit, waarbij respondenten de doelgroep vooral koppelen aan Whatsapp-fraude en spoofing.

Tabel 4. onderbouwing slachtofferschap per doelgroep

Relevante doelgroep	Toelichting
Ouderen	- Hebben te weinig digitale vaardigheden en kunnen veranderingen in techniek niet bijhouden - Hebben moeite onderscheid te maken tussen wat veilig en onveilig is - Hebben teveel vertrouwen / zijn te goedgelovig - Ze zijn een aantrekkelijk doelwit met relatief veel financiële middelen - Moeten zich tegen willen in online bevinden
Jongeren	- Kunnen minder goed de consequenties van diens gedrag overzien - Experimenteren van nature en nemen risico's - Zijn relatief makkelijk te manipuleren - Hebben niet veel geld tot hun beschikking, maar willen dat wel
Mensen van de middelbare leeftijd	- (Zie categorie 'iedereen')
Mkb	- Cybersecurity is ondergeschoven kindje: gebrek aan prioriteit - Onwetend van risico's en kwetsbaarheden - Investeren niet in maatregelen
Iedereen	- Beperkte computervaardigheden - Gebrek aan kennis - Naïviteit - Daders lopen voor - Gemakzucht

"Je kunt het wel proberen uit te leggen maar als ik alleen al het woord cyber gebruik, nou dan wordt men bang en dan horen ze ook niet meer de rest wat ik uit te leggen heb en dan wordt het te ingewikkeld." - EXP11

Jongeren zijn als tweede genoemd als veelvoorkomende slachtoffergroep. De bovengrens wordt hierbij vaak gelegd bij 24 jaar (EXP9 en EXP14). Uit de interviews komt naar voren dat bij deze groep online zedendelicten een belangrijke rol spelen, zoals grooming, sexting en sextortion (EXP1, EXP9, EXP12, EXP14). Extra kwetsbaar zijn wellicht jongeren die relatief snel naaktbeelden delen en gevoelig zijn voor manipulatie, waarbij lvb'ers en kinderen van gescheiden ouders zijn genoemd. Ook stellen respondenten dat dergelijke delicten in het bijzonder een hoge impact hebben op meisjes met een islamitische achtergrond (EXP12 en EXP14).
Jongeren zijn een kwetsbare groep volgens respondenten omdat ze – aangezien hun

"Volgens experts zijn de meest relevante doelgroepen om de cyberweerbaarheid van te verhogen: jongeren, ouderen, mensen van middelbare leeftijd en mkb'ers."

hersenen nog in ontwikkeling zijn - minder goed de consequenties van hun gedrag kunnen overzien, meer risico's nemen, experimenteren en op zoek zijn naar spanning (EXP9). Ze hebben ook vaak geldgebrek en zijn daarom over het algemeen gevoelig voor het verdienen van snel geld, aldus EXP3.
Om die redenen is volgens respondenten zowel daderschap als slachtofferschap onder jongeren hoog, zoals bij het doorsturen van naaktfoto's en het optreden als geldezel (EXP2, EXP5 en EXP14).
"Dus als je het hebt over preventief burgers, jongeren weerbaar maken door ze ervaren te maken, door ze te vertellen waar ze op moeten letten, wat de risico's zijn, hoe ze daarmee om kunnen gaan, ik zou ook absoluut werk maken van het feit dat bepaalde dingen gewoon echt niet mogen. Want in die groep wordt daar zoveel geëxperimenteerd zonder dat men doorheeft dat dat een sociale, een sociaal emotionele grens overgaat, maar ook juridische en criminele grenzen overgaat. Dus dat aspect vind ik wel van belang als je het hebt over cyberweerbaarheid." - (EXP12)
Een vrij brede doelgroep die is genoemd door respondenten betreft mensen van middelbare leeftijd. Zo geeft de politie aan dat het aantal aangiftes het hoogste is in de groep 35 tot 60 jaar (EXP1). Dit gaat vooral om financiële cyberdelicten. EXP9 herkent dat het aantal slachtoffers het hoogste is bij de groep 24 tot 44 jaar, waarbij online fraudes het meeste worden gemeld. Zo is Whatsapp-fraude een delict waarbij daders zich voordoen als kind van het slachtoffer, dus slachtoffers van dat delict zijn vaak 40 jaar of ouder (EXP1). Verklaringen voor slachtofferschap zijn vergelijkbaar met die van de algemene populatie, aangezien beide brede doelgroepen zijn, waarbij onder meer gemakzucht en een gebrek aan kennis zijn genoemd.
"Ja, ik denk dat het onoplettendheid is vooral. Niet voldoende nadenken. Je krijgt een mailtje van de bank. Even snel. Terwijl als je had nagedacht had je gezien misschien dat het een raar mailtje is of dat er iets niet helemaal klopt. We horen vaak wel van mensen, heb zijn net die momenten." - (EXP6)
Verder is het mkb aangedragen als relevante slachtoffergroep. Hoewel grote bedrijven ook slachtoffer kunnen worden, hebben die hun cybersecurity over het algemeen meer op orde (EXP2). Bij het mkb zou cybersecurity vaak 'een ondergeschoven kindje' zijn en het aan kennis ontbreken. Medewerkers zouden bovendien de tools missen om veilig te handelen, leidinggevenden zouden niet het goede voorbeeld geven en ondernemers zouden zichzelf niet als doelwit beschouwen. Investeringen in maatregelen blijven dan ook uit (EXP2, EXP7, EXP8, EXP10). Echter beschikken veel ondernemingen wel over gevoelige data die aantrekkelijk is voor criminelen. Genoemde voorbeelden zijn advocatenkantoren, notariskantoren of webshops met veel klantengegevens (EXP7). Ook mkb'ers die veel gebruik maken van technische apparatuur lopen risico op bepaalde vormen van cybercrime, zoals hacking en ransomware.

5.2.2. Meest voorkomende typen cybercrime volgens experts

In deze paragraaf zal uiteen gezet worden welke cyberdelicten volgens de experts het meest voorkomen. Tabel 5 toont een overzicht van die delicten. De experts hebben over het algemeen meerdere typen cybercrime aangemerkt.

Typen cybercrime	Aantal keer genoemd
phising	8 (EXP1, EXP2, EXP4, EXP6, EXP7, EXP8, EXP9 en EXP11)
ransomware	7 (EXP1, EXP4, EXP5, EXP7, EXP8, EXP10 en EXP11)
Whatsapp-fraude	7 (EXP1, EXP4, EXP5, EXP7, EXP8, EXP10 en EXP11)
Hacking	5 (EXP3, EXP10, EXP11, EXP12 en EXP14)
Sextortion / ssexting	3 (EXP3, EXP12 en EXP14)
Spoofing	3 (EXP4, EXP15 en EXP16)
D DoS-aanval	2 (EXP2 en EXP11)
factuurfraude	2 (EXP1 en EXP4)
Marktplaatsfraude / aan- en verkoopfraude	2 (EXP9 en EXP16)
Geldezel	2 (EXP3 en EXP5)
Helpdeskfraude	2 (EXP3 en EXP5)
Account take-overs	1 (EXP1)
Datingfraude	1 (EXP15)
Malafide Webshops	1 (EXP16)
CEO fraude	1 (EXP7)

Tabel 5. Meest voorkomende typen cybercriminaliteit volgens experts (N=15)

Meer dan de helft van de respondenten (N=8) geeft op basis van aangiftes en meldingen van slachtoffers aan dat phishing het meest voorkomende type cyberdelict is. Kanttekening hierbij is dat dit een brede categorie is, waarbij slachtofferschap vaak gepaard gaat met slachtofferschap van andere cyberdelicten, zoals het hacken van een internetbankierenaccount (EXP1). Daarnaast zijn niet alle melders ook daadwerkelijk slachtoffer en zijn de individuele schadebedragen vaak relatief klein (EXP4 en EXP6), wat het delict mogelijk minder urgent maakt dan de cijfers doen vermoeden. Phishing is volgens de experts niet gebonden aan een specifieke doelgroep: het komt bijvoorbeeld bij elke leeftijdscategorie voor. Bepaalde vormen van phishing zijn wel relevant voor specifieke doelgroepen, zoals business e-mail compromise in het geval van het mkb. Ransomware en Whatsapp-fraude worden door de experts beide zeven keer aangedragen. Het aantal aangiftes van ransomware is relatief laag, maar respondenten herkennen op basis van meldingen van slachtoffers en externe rapporten dat het veel voorkomt onder het mkb en ook toe lijkt te nemen (EXP1, EXP4, EXP4, EXP8 en EXP10). Respondenten durven niet te zeggen hoe het komt dat slachtoffers niet naar de politie gaan; mogelijk denken slachtoffers dat aangifte doen geen zin heeft (EXP1). Verder beschrijft EXP1

dat ransomware-aanvallen steeds gerichter worden.

"Dus dat die ransomware niet meer het internet op geslingerd wordt en iedereen kan slachtoffer worden, maar dat ze vaker een gericht doelwit pakken. En of dat nou een prominent persoon is of een organisatie, ja dat kan allebei." - (EXP1)

In het geval van Whatsapp-fraude doen daders zich bijvoorbeeld voor als zoon of dochter van het slachtoffer, zo blijkt uit de interviews (EXP1, EXP4 en EXP6). Dit delict nam het afgelopen jaar sterk toe onder de doelgroep ouderen. Volgens twee respondenten hebben er mogelijk datalekken plaatsgevonden bij bedrijven of is er op voorhand sprake van phishing, waardoor criminelen beschikken over persoonlijke gegevens van ouderen en zij gericht een aanval kunnen uitvoeren (EXP4 en EXP6). Zo gaan er op het Dark Web ook lijsten rond met contactgegevens van ouderen, aldus de respondenten (EXP4 en EXP6).
Hacking is vijf keer genoemd als veelvoorkomend delict. In twee gevallen heeft dit betrekking op de doelgroep mkb, zoals het hacken van apparatuur en het stelen van bedrijfsgegevens. De andere drie respondenten geven aan dat hacking veel voorkomt onder jongeren. Bij jongeren gaat het met name om het hacken van social media accounts voor het verkrijgen van persoonlijke foto's. Volgens twee respondenten is hacking echter een containerbegrip dat beschouwd dient te worden als een middel in plaats van een delict (EXP1 en EXP7). Ook EXP2 herkent dat hacking als zelfstandig delict niet vaak voorkomt, hoewel er ook sprake kan zijn van onderrapportage, omdat veel gevallen zich in de interpersoonlijke sfeer afspelen en niet worden gemeld.

"Dus stel dat wij naast elkaar wonen en we krijgen ruzie, voorheen gooide ik een plant bij jou in de tuin, maar nu ga ik je facebookpagina hacken, dus je ziet natuurlijk dat dat soort delicten ook massaal voorkomen, alleen daar wordt relatief weinig aangifte van gedaan." - (EXP2)

Sexting en sextortion zijn driemaal benoemd als meest voorkomende delicten. Dit wordt over het algemeen genoemd in het kader van de doelgroep jongeren, hoewel ook oude mannen slachtoffer worden van afpersing met naaktbeelden (EXP1). Over de daadwerkelijke omvang is weinig bekend, omdat jongeren er niet zo gauw melding van maken, aldus een jongerenwerker. Experts verwachten op basis van bijvoorbeeld signalen vanuit scholen dat het vaak voorkomt. Verder is ook spoofing drie keer genoemd door respondenten. Dit delict vertoont gelijkenissen met Whatsappfraude: beide vormen zijn specifiek gericht op ouderen en nemen recentelijk sterk toe. Spoofing heeft in dit geval betrekking op criminelen die zich (telefonisch) voordoen als een bankmedewerker om slachtoffers te misleiden tot het overmaken van geld.

"Weet je, het vervelende bij spoofing is dat je vertrouwen ook enorm geschaad is." - (EXP15)

Een aantal delicten zijn één- of tweemaal aangedragen als meest voorkomend. DDoS-aanvallen, factuurfraude en CEO-fraude hebben primair betrekking op de doelgroep mkb. Met name factuurfraude lijkt de laatste jaren redelijk veel aanwezig en heeft relatief hoge schades (EXP1 en EXP4). Ook Marktplaatsfraude en malafide webshops komen in het algemeen veel voor volgens EXP9 en EXP16. Verder lijkt het fenomeen geldezels een groeiend probleem te worden, met name onder jongeren, aldus tweeorganisaties (EXP3 en EXP5). Hierbij is de lijn tussen slachtofferschap en daderschap dun. Ten slotte zijn helpdeskfraude en datingfraude genoemd voor de doelgroep ouderen. Zo geeft EXP6 aan dat helpdeskfraude de laatste tijd weer toeneemt, waarbij in sommige gevallen mensen zelf contact zoeken met een bedrijf omdat zij via een nepwebsite bij oplichters terecht komen. In het geval van datingfraude zijn de schades en de persoonlijke en financiële impact vaak zeer groot, aldus EXP15.

5.2.3. Meest prominente doelgroepen en typen cybercrime volgens experts

Ter verdieping op de meest voorkomende typen cybercrime en slachtoffergroepen, is gevraagd naar de meest noodzakelijke typen cybercrime en slachtoffergroepen om de cyberweerbaarheid van te verhogen. Het is echter gebleken dat experts geen specifieke groepen of delicten aanwezen. Zo zijn de meeste experts op het gebied van slachtoffergroepen van mening dat iedereen slachtoffer wordt
van cybercriminaliteit en dat de noodzakelijke doelgroep afhankelijk is van het type cybercrime (EXP1, EXP2, EXP3, EXP5, EXP6 en EXP9).
"Je gaat een aantal subboodschappen brengen, en afhankelijk van of dat nou over een helpdeskfraude gaat, over phishing of over sextortion, zou ik mijn doelgroep daarop afstemmen." - (EXP1)

Op basis van de interviews ontstaat er een beeld wat betreft deze koppeling tussen doelgroep en delict. Zo lijken voor de doelgroep ouderen met name spoofing en Whatsapp-fraude relevant (EXP4, EXP6 en EXP15). Beide delicten zijn volgens de respondenten specifiek gericht op ouderen en zowel de omvang als de financiële en persoonlijke impact op slachtoffers is groot. Zo hebben de delicten binnen de categorie fraude relatief hoge schadebedragen (EXP6). De respondenten zien in het geval van jongeren met name belang in interpersoonlijke delicten, waarbij sextortion vaak ter sprake is gekomen, ondanks dat het relatief lastig is om zicht te krijgen op dat delict. Hierbij lijkt dan ook vooral de hoge impact op slachtoffers een belangrijke afweging. Gerelateerd hieraan is het hacken van (social media) accounts, zoals Instagram en iCloud: het gehackte beeldmateriaal wordt gebruikt om slachtoffers te bedreigen of af te persen voor geld (EXP14).

"Ik lees verhalen van slachtoffers die dus gewoon maanden niet meer het huis uit durfden, alleen maar omdat hun snapchat account gehackt was." - (EXP3)

Voor de doelgroep mkb lijken respondenten technische cyberdelicten als meest relevant te beschouwen; in het bijzonder ransomware. Naast de hoge omvang onder de doelgroep, kan het ook grote gevolgen hebben voor bedrijfsprocessen en gaat het gepaard met hoge financiële schade (EXP10 en EXP11). Het kan een bedrijf helemaal stilleggen en slachtoffers overzien de kosten vaak niet, aldus EXP10. Ten slotte lijkt over de gehele breedte phishing te worden beschouwd als meest relevante cybercrime:

phishing is niet gebonden aan een specifieke doelgroep, heeft de grootste omvang en gaat in totaliteit gepaard met de hoogste financiële schade (EXP1 en EXP4).
Naast de specifieke delicten en doelgroepen, zien respondenten ook relevantie in andere strategieën. Zo is het volgens EXP8 van belang om preventief de technische beveiliging te vergroten, zodat mensen zelf minder hoeven te doen. Een politiemedewerker geeft aan dat financieel- economisch gedreven cybercriminaliteit in het algemeen de aandacht verdient: criminelen willen geld verdienen, ongeacht de specifieke wijze.
Een cybersecuritybedrijf stelt dat, hoewel zij vaak meldingen krijgen van vormen van online fraude, er niet één het meest noodzakelijk is: mensen moeten in het algemeen meer cyberweerbaar worden (EXP7). Genoemde voorbeelden zijn het gebruik van 2-factor authenticatie en sterkere wachtwoorden. EXP7 vindt in die overtuiging steun van drie andere experts (EXP6, EXP14 en EXP5).
Verder zijn twee respondenten van mening dat het zaak is om te anticiperen op toekomstige cybercrimevormen (EXP12 en EXP16). Tegen de tijd dat mensen doorhebben hoe Whatsapp-fraude werkt, is er alweer wat nieuws verzonnen, zo haalt EXP16 aan als voorbeeld. Met het oog op de toekomst lijkt er op basis van de interviews een opvallend beeld te ontstaan: de meeste respondenten zien vooral gevaar in nieuwe technologische ontwikkelingen en cybercrimevormen die daarmee gepaard gaan, waarbij onder meer 'deepfakes', drones en IoT expliciet zijn benoemd (EXP1, EXP4, EXP6, EXP7, EXP12, EXP15 en EXP16). Dergelijke ontwikkelingen zorgen voor nieuwe kansen voor criminelen en verschuivingen in slachtofferschap, hoewel nog steeds in potentie iedereen slachtoffer kan worden (EXP1).

"Ik hoor nu de politie al zeggen dat deepfake nu nog minuscuul is, maar dat ze al voorbeelden zien van jongeren die daarmee spelen. En daar maak ik me wel zorgen over. Daar moet je nu in feite al op anticiperen, dat die beelden... Want je kunt er vergif op innemen dat 96 procent van de vrouwen daar straks het slachtoffer van is." - (EXP12)

Volgens de experts is het verhogen van de cyberweerbaarheid per doelgroep vooral van belang bij de volgende typen cyberdelicten:

1) Jongeren: interpersoonlijke cyberdelicten, met name shame sexting / sextortion
2) Ouderen: financiële cyberdelicten, met name vriend-in-noodfraude en spoofing
3) Mkb'ers: technische cyberdelicten, met name ransomware
Daarnaast komt naar voren dat phishing een belangrijk cyberdelict is, waarbij van iedereen de cyberweerbaarheid verhoogd moet worden.
Aandacht wordt gevraagd voor geldezelen; dit is sterk in opkomst, met name onder jongeren, waarbij de scheidslijn tussen dader- en slachtofferschap dun is.

5.3. Deelconclusie inzichten uit de praktijk

Voor welke doelgroepen zijn interventies om het risicobewustzijn en het preventieve gedrag te vergroten het meest noodzakelijk? Op basis van de inzichten die verkregen zijn uit de interviews met zowel gemeenten als andere experts op het gebied van cybercriminaliteit, komt een redelijk eenduidig beeld naar voren. De drie doelgroepen die als meest relevant en kwetsbaar door beide groepen genoemd zijn, zijn:

1. Jongeren
2. Mkb'ers
3. Ouderen/senioren

Opvallend is, dat alle ondervraagde gemeenten aangeven dit (deels) te baseren op geregistreerde cijfers van bijvoorbeeld de politie of het CBS. Tegelijkertijd geven zij aan, dat deze cijfers volgens hen niet volledig zijn en te weinig houvast geven om harde beleidsadviezen op te bouwen. Daarom nemen zij naast de cijfers, ook de ernst en omvang van de impact van een cyberdelict op de slachtoffers mee in hun overwegingen. Officiële cijfers over slachtofferschap van cybercriminaliteit lijken dus tot nu toe beperkt bruikbaar voor gemeenten, omdat ze een onjuist beeld schetsen van de werkelijkheid en weinig handelingsperspectief bieden. De helft van de gemeenten geeft dan ook aan inschattingen over slachtofferschap te baseren op anekdotisch materiaal, zoals gevoel, 'gezond verstand' of signalen en verhalen uit de omgeving. Door experts wordt de keuze onderbouwd door gegevens die zij in hun eigen praktijk gebruiken of zelf registreren.

Een ander punt is dat de definiëring van de doelgroepen verschilt per gemeente. Zo zijn er gemeenten die de doelgroep jongeren benaderen vanuit de leeftijd van 8-30 jaar, terwijl anderen hier een beperktere leeftijd hanteren van jongeren tot 18 jaar.
De onderbouwing voor keuze van doelgroepen vertoont wel een gedeeld patroon onder gemeenten en experts: jongeren worden genoemd, omdat zij veel online zijn, zich (nog) niet bewust zijn van de risico's en effecten en vanwege de impact die cyberdelicten op hun leven hebben. Mkb'ers worden vooral genoemd als potentiële doelgroep door de mogelijke financiële gevolgen een rol, waar voor ouderen/senioren vooral de lage cyberweerbaarheid, gebrek aan bewustzijn en goed vertrouwen de onderbouwing zijn voor het positioneren als relevante doelgroep.
Voor welke typen cybercrime zijn interventies om het risicobewustzijn en het preventieve gedrag van deze doelgroepen te vergroten het meest noodzakelijk?
Wat betreft de typen cybercriminaliteit waarop cyberweerbaarheidsbevordering zich volgens gemeenten op zou moeten richten, is ook een gevarieerd beeld waargenomen. De meest genoemde zijn:

1. Shame sexting (N=7)
2. Phishing (N=4)
3. Vriend-in-nood fraude/ Aan- en verkoopfraude / Malware / DDoS-aanvallen (N=3)

De motivatie hiervoor is verschillend. Bij shame sexting gaat het met name om de impact die het delict heeft op het leven van de (veelal jonge) slachtoffers. Phishing is volgens de respondenten een veelvoorkomende vorm van cybercriminaliteit, waarvan iedereen in principe slachtoffer kan worden en

daarom relevant is. Bij malware/ransomware worden vooral de financiële gevolgen voor ondernemers genoemd. De vriend-in-nood-fraude wordt vooral gekoppeld aan een specifieke doelgroep: de ouderen/senioren en de prevalentie van dit delict onder deze doelgroep.
Dit komt gedeeltelijk overeen met het beeld dat geschetst wordt door de geïnterviewde experts. De meest voorkomende delicten zijn volgens de experts:
1. Phishing (N=8)
2. Ransomware / vriend-in-noodfraude (N=7)
3. Hacking (N=5)

Desgevraagd hebben experts aangegeven welke delicten het meest relevant zijn binnen de hierboven beschreven doelgroepen. Zij zien bij jongeren met name *interpersoonlijke cyberdelicten* als relevant om het risicobewustzijn en de cyberweerbaarheid voor te verhogen. Hierbij worden shame sexting en sextortion als belangrijkste specifieke delicten aangemerkt. Een uitzondering hierop is het delict geldezelen, een delict dat volgens experts sterk in opkomst is en waarbij slachtofferschap en daderschap door elkaar heen lopen[23]. Bij ouderen/senioren komen hierbij met name *financiële cyberdelicten* naar voren, waarbij vriend-in-noodfraude en spoofing het meest worden genoemd.
De keuze om deze delicten als noodzakelijk aan te merken lijkt te berusten op zowel de omvang als de impact van de delicten op de slachtoffers. Bij mkb'ers worden door experts, net als door gemeenten, phishing en verschillende technische cyberdelicten genoemd, zoals ransomware, hacking en DDoS- aanvallen.
Op basis van de twee interviewrondes met gemeentelijke functionarissen en experts uit het werkveld van cybercriminaliteit, is het beeld – wanneer relevante doelgroepen en typen cyberdelicten waarvoor zij vatbaar zijn worden gekoppeld – als weergegeven in Tabel 6, waarbij per doelgroep één specifiek delict is aangegeven waarvoor deze groep extra vatbaar lijkt te zijn.

23 De geldezel (die soms denkt geen risico te lopen omdat er geen saldo op de rekening staat, waardoor er niet meer kan worden opgenomen dan er eerst op is overgemaakt) is aansprakelijk voor het doorgesluisde geld, bijvoorbeeld als onverschuldigde betaling. Geldezels kunnen strafrechtelijk worden vervolgd voor medeplichtigheid aan oplichting. Als hij had moeten begrijpen dat hij een crimineel hielp is hij ook strafbaar. Een naïeve geldezel is ook te beschouwen als slachtoffer.

Tabel 6. Overzicht doelgroepen en bijbehorende delicten volgens gemeenten en experts

Doelgroep	Delict
Jongeren	-Shame sexting / sextortion -Geldezelen
Ouderen	Vriend-in-noodfraude
Mkb'ers	Malware

5.4. Toetsing deelconclusie aan praktijkpartners

Aanvullend zijn de resultaten van de twee interviewrondes getoetst aan de kennis en inzichten van lokale partners van de deelnemende gemeenten. Deze praktijkpartners werken dagelijks met de betreffende doelgroepen. De gemeentelijke consortiumpartners hebben met behulp van een korte vragenlijst (Bijlage 4) de bevindingen uit de interviews voorgelegd aan deze praktijkpartners om te verifiëren of zij de prominente doelgroepen en bijbehorende delicten waarvan zij slachtoffer worden, herkennen vanuit hun dagelijkse werk met deze doelgroepen. Deze aanvullende inzichten worden hieronder per doelgroep voor het meest prominente delict (jongeren: shame sexting/ sextortion, ouderen: vriend-in-noodfraude en mkb'ers: malware) besproken.

5.4.1. Jongeren

Het overgrote deel van de praktijkpartners geeft aan dat bij jongeren shame sexting een veelvoorkomend delict is. Hierbij wordt aangegeven dat het vooral onderdeel is van laster en pesten. Sextortion (waarbij slachtoffers worden afgeperst naar aanleiding van seksueel getint beeldmateriaal) wordt door deze partijen minder vaak gezien.
Zij zien dat meisjes het vaakst slachtoffer worden, waarbij twee subgroepen in het bijzonder worden aangemerkt als kwetsbaar. Ten eerste meisjes met een migratieachtergrond (specifiek islamitische), omdat bij deze groep de integriteit en de relatie met normen en waarden over seksueel gedrag een grote rol spelen. Ten tweede zijn slachtoffers volgens respondenten vaak onzekere en naïeve meisjes, die 'er graag bij willen horen' en daardoor makkelijker over hun eigen grenzen gaan. De praktijkpartners geven aan dat de impact van shame sexting en sextortion enorm is voor de slachtoffers. Dit heeft met name betrekking op de mentale en sociale gevolgen, waarbij depressies, zelfmoord(intenties), negatief zelfbeeld, het

vermijden van sociale contacten en toename van verslavingen als belangrijkste en veelvoorkomende gevolgen worden genoemd.

5.4.2. Ouderen

De praktijkpartners hebben een minder eenduidig beeld over de prevalentie van vriend-in-noodfraude bij ouderen. Ongeveer de helft geeft aan dit te herkennen als een vorm van oplichting die vaak voorkomt bij ouderen, terwijl de andere respondenten dit niet direct herkennen. Respondenten die in hun dagelijkse werk zien dat ouderen slachtoffer worden van Whatsapp-fraude, geven aan dat de impact op slachtoffers tweeledig is. Ten eerste is er de financiële schade, wanneer zij geld overgemaakt hebben. Daarnaast heeft slachtofferschap invloed op het eigen vertrouwen in digitale vaardigheden, waarbij vooral de angst om devices te gebruiken toeneemt na slachtofferschap. De oorzaken van slachtofferschap volgens de praktijkpartners liggen enerzijds in de beperkte digitale vaardigheden en kennis van de doelgroep; anderzijds lijkt ook hier naïviteit een rol te spelen; slachtoffers zijn goed van vertrouwen en er wordt een appèl gedaan op hun bereidheid een bekende of familielid te helpen.

5.4.3. Mkb'ers

De meeste ondervraagde praktijkpartners herkennen dat malware een delict is waar mkb'ers slachtoffer van worden. Eén respondent geeft aan dat mkb'ers daar wel slachtoffer van worden, maar dat er weinig duidelijkheid bestaat over aantallen, omdat velen het niet melden of er niet over spreken. Hierdoor is er bij de praktijkpartners ook weinig inzicht in de schade die deze doelgroep oploopt als gevolg van malware. Vermoedens zijn dat het vooral gaat om financiële schade en het verlies van gegevens en data. Volgens de respondenten wordt slachtofferschap veroorzaakt door een gebrek aan kennis en middelen. Daarnaast speelt bij mkb'ers vaak mee dat niemand in het bedrijf verantwoordelijk is voor IT, waardoor – in combinatie met gebrek aan kennis – de systemen en gegevens onvoldoende beschermd zijn tegen malware. Een respondent benoemt dat voor mkb'ers automatisering vaak wordt gezien als een 'noodzakelijk kwaad', waardoor er te weinig tijd en aandacht is voor cyber security en er bijvoorbeeld ook geen back-ups worden gemaakt van bestanden, waardoor de impact groot kan zijn voor mkb'ers.

6. CONCLUSIE

Op basis van de resultaten worden in dit hoofdstuk de onderzoeksvragen beantwoord. In paragraaf 6.1 wordt ingegaan op de meest prominente doelgroepen voor het verhogen van cyberweerbaarheid, waarna in paragraaf 6.2 wordt in gegaan op de meest prominente typen cybercriminaliteit. In 6.3 wordt vervolgens besproken hoe de doelgroepen en delicten aan elkaar gekoppeld zouden kunnen worden. Paragraaf 6.4, tenslotte, geeft een overkoepelende conclusie met de keuze voor de drie prominente doelgroepen en bijbehorende typen cyberdelicten waarvoor het vergroten van het risicobewustzijn en de cyberweerbaarheid het meest noodzakelijk is.

6.1. Doelgroepen

De eerste onderzoeksvraag van dit rapport was: *"Voor welke doelgroepen zijn interventies om het risicobewustzijn en het preventieve gedrag te vergroten het meest noodzakelijk?"*
Deze vraag is beantwoord op basis van twee onderzoeksmethoden; een literatuurstudie en interviews.
Tijdens de literatuurstudie kwam naar voren dat er geen eenduidig risicoprofiel is voor slachtoffers van cybercriminaliteit. Studies gericht op de samenhang tussen verschillende kenmerken en slachtofferschap concludeerden dat er zeer beperkte verbanden zijn tussen factoren als geslacht, opleidingsniveau en sociaal economische status en het risico op slachtofferschap van cybercriminaliteit.
Toch zijn uit de literatuurstudie wel twee groepen naar voren gekomen die een verhoogd risico lijken te hebben; jongeren en mkb'ers (midden- en klein bedrijf). Jongeren lijken vooral een verhoogd risico te lopen op *interpersoonlijke cyberdelicten,* zoals stalking, bedreiging met geweld en laster. Mkb'ers lijken verhoogd risico te lopen op zowel *financiële* als *technische cyberdelicten*, zoals phishing, hacking en malware.
Op basis van de resultaten van de interviews met zowel gemeentelijke functionarissen op het gebied van cybercriminaliteit als de overige experts uit het vakgebied, zijn drie prominente doelgroepen naar voren gekomen: jongeren, ouderen en mkb'ers.
De respondenten waren hier in zijn algemeenheid eensgezind. Deze groepen komen overeen met de twee groepen die uit de literatuurstudie naar voren kwamen (jongeren en mkb'ers) en er is een nieuwe groep toegevoegd: ouderen. De experts duiden ouderen zelfs aan als de meest prominente groep. Deze groep is door de gemeentelijke functionarissen en experts aangemerkt als prominente risicogroep omdat deze groep kwetsbaar zou zijn vanwege hun beperkte digitale vaardigheden en dat zij een aantrekkelijk doelwit zijn met relatief veel financiele middelen. Dat maakt bovendien dat de impact van slachtofferschap potentieel zeer groot kan zijn.
Het aanmerken van deze risicogroepen als het meest prominent voor het verhogen van cyberweerbaarheid wordt op verschillende manieren onderbouwd. Zo wordt door de gemeenten gebruik gemaakt van cijfers (zoals politiecijfers en CBS-cijfers) als input voor beleidsvorming, maar er wordt tegelijkertijd aangegeven dat cijfers geen volledig beeld en te weinig houvast bieden. Daarom prioriteren gemeenten ook op basis van 'wat

zij horen in de samenleving' en de ernst en omvang van de impact van slachtofferschap (bijvoorbeeld financieel of emotioneel) voor doelgroepen. Experts baseren zich, naast officiële cijfers, ook op de signalen en registraties uit hun eigen dagelijkse beroepspraktijk.
Een relevant resultaat dat van belang is toe te voegen aan het lijstje met meest prominente doelgroepen, is dat veel gemeenten en experts aangaven dat het vergroten van het risicobewustzijn en de cyberweerbaarheid in zijn algemeen voor iedereen in de maatschappij van groot belang is. Cybercriminaliteit wordt in die zin gezien als gemeengoed: iedereen is tegenwoordig online en daarmee een potentieel slachtoffer. Daarnaast zijn sommige cyberdelicten – zoals phishing, hacking en aankoopfraude – niet per sé doelgroepspecifiek, maar gerelateerd aan risicovolle gedragingen onder (bijna) alle eindgebruikers.
Samengenomen wijzen de resultaten van dit rapport op drie risicogroepen voor wie het verhogen van hun cyberweerbaarheid het meest noodzakelijk is:
1) jongeren
2) ouderen
3) mkb'ers

6.2. Typen cyberdelicten

De tweede onderzoeksvraag van dit rapport was: *"Voor welke typen cybercrime zijn interventies om het risicobewustzijn en het preventieve gedrag van deze doelgroepen te vergroten het meest noodzakelijk?"* Ook deze vraag zal worden beantwoord op basis van twee onderzoeksmethoden; een literatuurstudie en interviews.
In dit onderzoek zijn cyberdelicten ingedeeld op basis van *technische, financiële en interpersoonlijke cyberdelicten.* Binnen de drie categorieën is op basis van de literatuur een aantal delicten aangewezen als de meest voorkomende delicten en daarmee de delicten waarvoor het vergroten van cyberweerbaarheid bij potentiële slachtoffers het meest noodzakelijk is. Concluderend kan worden gesteld, dat binnen de *technische cyberdelicten* dit malware en hacking zijn; in de categorie *financiële cyberdelicten* zijn dit phishing, aankoopfraude en identiteitsfraude, en binnen de interpersoonlijke delicten zijn dit laster, chantage, stalking en bedreiging met geweld (al dan niet met een seksuele (bij)bedoeling).
Tijdens de interviews met vertegenwoordigers van gemeenten en experts in het veld van cybercriminaliteit en cyberweerbaarheid zijn verschillende delicten aangewezen als de meest prominente delicten om cyberweerbaarheid tegen te verhogen onder potentiële slachtoffers. Hoewel de delicten die respectievelijk de gemeenten en de experts aanwezen niet volledig overeenkomen, zijn er samengenomen vijf prominente delicten aan te wijzen, zijnde:
1. Phishing
2. Shame sexting/sextortion
3. Malware/Ransomware
4. Vriend-in-nood
5. Geldezelen

Ook hier dient opgemerkt te worden dat het beeld niet altijd eenduidig is. Hieraan kunnen een aantal redenen ten grondslag liggen. Ten eerste treden deze delicten niet altijd afzonderlijk van elkaar op: phishing of hacking, bijvoorbeeld, gaan vaak vooraf aan het plegen van identiteitsfraude. Slachtofferschap is dus vaak een gevolg van een serie aan delicten. Zo kan iemand slachtoffer worden van identiteitsfraude of ransomware vanwege een eerdere geslaagde phishingaanval.
Ten tweede blijkt zowel uit de literatuurstudie als de interviews dat de beschikbare cijfers een onvolledig beeld schetsen, doordat niet iedereen aangifte of een melding doet, niet iedereen zich bewust is van slachtofferschap en dat niet alle cyberdelicten als zodanig worden geregistreerd door de politie. Mede daardoor verschillen in sommige gevallen de cijfers van de incidenten die experts tegen komen in de praktijk en die gemeentefunctionarissen bereiken.
Ten derde blijkt uit de interviews dat de motivatie voor prioritering van typen cybercriminaliteit verschilt tussen gemeenten. In sommige gevallen is een delict aangemerkt als prominent binnen een bepaalde doelgroep, maar in andere gevallen geven zij aan dat er vormen van cybercriminaliteit zijn waarbij iedereen in principe slachtoffer kan worden, waardoor deze als relevant worden aangemerkt (zoals phishing en aan- en verkoopfraude). Ook is uit de interviews, alsmede uit de discussiebijeenkomsten duidelijk geworden dat ontwikkelingen in slachtofferschap van cybercriminaliteit en de prevalentie van typen delicten aandacht vragen. Met name geldezelen is naar voren gekomen als een type cyberdelict dat sterk in opkomst is; vooral gekoppeld aan de doelgroep jongeren. Kenmerkend voor geldezelen is, dat de scheidslijn tussen dader- en slachtofferschap in sommige gevallen dun is[24].

6.3. Koppeling delicten en doelgroepen

Op basis van de keuze van de meest prominente doelgroepen (6.1) en cyberdelicten (6.2) is vervolgens een inventarisatie gedaan naar de meest prominente typen cyberdelicten binnen elke doelgroep.
Een eerste bevinding is dat zowel de literatuur als de resultaten uit de interviews lijken te wijzen naar een duidelijke koppeling tussen categorieën cybercriminaliteit en doelgroepen. Voor de doelgroep jongeren komt de categorie *interpersoonlijke cyberdelicten* het meest prominent naar voren. Bij de doelgroep mkb'ers komt met name de categorie *technische cyberdelicten* naar voren. Op basis van de resultaten uit de interviews komt een koppeling naar voren tussen ouderen en *financiële cyberdelicten*.
Vervolgens is gekeken of er een koppeling kon worden gemaakt tussen specifieke cyberdelicten en doelgroepen. Opvallend was dat een dergelijke koppeling door verschillende experts uit zichzelf werd gemaakt.
De meest prominente cyberdelicten (6.2) werden bijvoorbeeld diverse malen specifiek binnen een bepaalde doelgroep aangemerkt. De doelgroep jongeren werd het vaakst aan shame sexting en sextortion gekoppeld. Mkb'ers lopen volgens gemeenten en experts het meest risico op slachtofferschap van een DDoS-aanval en malware (specifiek ransomware). Binnen de doelgroep ouderen kwam vooral vriend-in-noodfraude (Whatsapp-fraude) en spoofing naar voren. Naast de koppelingen tussen cyberdelicten en doelgroepen die naar voren gekomen zijn in deze studie, hebben diverse experts ook

24 De geldezel maakt het doorsluizen van frauduleus verkregen geld mogelijk en als hij had kunnen begrijpen dat hij een crimineel hielp is hij ook strafbaar voor medeplichtigheid aan oplichting. Een naïeve geldezel is echter ook te beschouwen als slachtoffer, omdat hij niet altijd kan weten dat hij meewerkt aan het doorsluizen van crimineel geld.

gewezen op prominente cyberdelicten die niet aan een specifieke doelgroep te koppelen zijn. Iedereen kan slachtoffer worden van dergelijke cyberdelicten. De experts benadrukken dan ook het belang van het verbeteren van algemene cyberweerbaarheid onder internetgebruikers. Phishing werd bijvoorbeeld het vaakst van alle cyberdelicten aangedragen door gemeentes en experts, maar werd over het algemeen niet gelinkt aan een specifieke doelgroep. De consensus onder respondenten lijkt te zijn dat iedereen slachtoffer van phishing kan worden. Ook hacking werd niet consequent gelinkt aan een bepaalde doelgroep, maar werd ongeveer even vaak aangemerkt onder jongeren als mkb'ers.

6.4. Keuze voor doelgroepen en typen cyberdelicten

Dit rapport sluit af met de keuze voor prominente doelgroepen voor het verhogen van cyberweerbaarheid en specifieke cyberdelicten waar toekomstige interventies zich op zouden moeten richten. De keuze voor de prominente doelgroepen is ontstaan door de inzichten uit zowel de literatuur als uit de interviews met gemeenten en experts te bundelen. De drie doelgroepen die zijn gekozen, zijn; jongeren, ouderen en mkb'ers. Vervolgonderzoek binnen deze groepen is nodig om de vraag te beantwoorden waarom juist deze groepen vaker slachtoffer worden van cybercriminaliteit.
In de afwegingen bij deze keuze voor specifieke cyberdelicten binnen deze doelgroepen is rekening gehouden met de prevalentie van cyberdelicten zoals die in de literatuur naar voren is gekomen, onderbouwingen in de keuze voor specifieke cyberdelicten door de respondenten en een eventuele consensus tussen de literatuur en de inzichten van de respondenten. Bovendien speelt ook de mate van impact van slachtofferschap van deze delicten een belangrijke rol. Hiermee is het aanmerken van een doelgroep gebaseerd op de combinatie van zowel de kans als de mogelijke impact.
Op basis van deze overwegingen is voor de doelgroep jongeren gekozen voor shame sexting / sextortion, voor de doelgroep ouderen voor vriend-in-noodfraude, en voor mkb'ers voor ransomware. Voor alle drie delicten laten de resultaten zien dat ze vaak voorkomen binnen deze groepen en dat de impact op slachtoffers ontzettend groot is. Ondanks dat er andere cyberdelicten zijn die nog vaker voorkomen, dienen deze drie cyberdelicten aangemerkt te worden als de meest noodzakelijke delicten om cyberweerbaarheid tegen te vergroten.
Daarnaast kan niet voorbij gegaan worden aan het meest prominente cyberdelict; phishing. Daar de resultaten erop wijzen dat voor phishing relevant is voor alle eindgebruikers en derhalve niet is verbonden aan een specifieke doelgroep, is dit delict gekozen voor alle drie de doelgroepen.
In Tabel 7 is de keuze van typen delicten per doelgroep, waarvoor het ontwikkelen van interventies ten behoeve van het vergroten van de cyberweerbaarheid het meest noodzakelijk is, weergegeven.

Tabel 7. Keuze voor de meest prominente doelgroepen en cyberdelicten

Doelgroep	Delict 1	Delict 2
Jongeren	Shame sexting/sextortion Geldezelen	Phising
Ouderen	Shame sexting/sextortion Geldezelen	Phising
Mkb	Ransomware	Phising

GERAADPLEEGDE LITERATUUR

Aïmeur, E., & Schőnfeld, D. (2011). The ultimate invasion of privacy: Identity theft. *2011 Ninth Annual International Conference on Privacy, Security and Trust*, 24-31. https://doi.org/10.1109/PST.2011.5971959

Alert Online (2019, 19 september). *Nationaal Cybersecurity Bewustzijnsonderzoek 2019.* https://www.alertonline.nl/media/Alert-Online-Cybersecuritybewustzijnsonderzoek-2019- 2.pdf

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security, 74*, 144-166. https://doi.org/10.1016/j.cose.2018.01.001

Anderson, K. B. (2006). Who Are the Victims of Identity Theft? The Effect of Demographics. *Journal of Public Policy & Marketing, 25*(2), 160–171. https://doi.org/10.1509/jppm.25.2.160.

Babchishin, K. M., Hanson, R. K., & Hermann, C. A. (2011). The characteristics of online sex offenders: A meta-analysis. *Sexual Abuse: A Journal of Research and Treatment, 23*(1), 92-123. https://doi.org/10.1177/1079063210370708

Bates, S. (2017). Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors. *Feminist Criminology, 12*(1), 22–42. https://doi.org/10.1177/1557085116654565

Beaming (2018). *Cyber threat report 2018*. https://www.beaming.co.uk/press releases/small-businesses-hit-hardest-by-17bn-cybercrime-bill-in-2018/

Beerthuizen, M. G. C. J., Sipma, T., & van der Laan, A. M. (2020). *Aard en omvang van dader-en slachtofferschap van cyber-en gedigitaliseerde criminaliteit in Nederland*. WODC. https://repository.wodc.nl/handle/20.500.12832/253

Björck F., Henkel M., Stirna J., Zdravkovic J. (2015). Cyber Resilience – Fundamentals for a Definition. In A. Rocha, A. Correia, S. Costanzo & L. Reis (Eds.), *New Contributions in Information Systems and Technologies* (pp. 311-316). Springer. https:// doi.org/10.1007/978-3-319-16486-1_31

Bloem, B. & Harteveld, A. (2012). *Horizontale fraude: Verslag van een onderzoek voor het Nationaal dreingsbeeld 2012* . Dienst IPOL. https://ultrascan-research.com/assets/files/ndb- horizontale-fraude-dreigingsbeeld-2012.pdf

Bossler, A. M., Holt., T.J. (2009). On-line activities, guardianship, and malware infection: an examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400-420.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38*(3), 227-236. https://doi.org/10.1016/j.jcrimjus.2010.03.001

Bossler, A. M., Holt, T. J. (2011). Malware victimization: A routine activities framework. In K. Jaishankar (Ed.), *Cyber criminology: Exploring internet crimes and criminal behavior*

(1, 317- 346). Taylor & Francis. https://doi.org/10.1201/b10718
Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security,* 2016(9), 5-9. https://doi.org/10.1016/S1353-4858(16)30086-1
Caputo, D. D., Burns, A. J. & Johnson, M.E. (2014). Going Spear Phishing: Exploring Embed ded Training and Awareness. *IEEE Security & Privacy, 12*(1), 28–38. https://doi. org/10.1109/MSP.2013.106
CBS. (2018a). *Veiligheidsmonitor 2017*. https://www.cbs.nl/nl- nl/publicatie/2018/09/veilig heidsmonitor-2017
CBS (2018b). *Cybersecuritymonitor 2018.* https://www.cbs.nl/nl- nl/publicatie/2018/38/cy bersecuritymonitor-2018
CBS. (2019, 17 juli). *Digitale Veiligheid & Criminaliteit 2018*. https://www.cbs.nl/nl- nl/publi catie/2019/29/digitale-veiligheid-criminaliteit-2018
CBS. (2020a, 2 maart). *Minder traditionele criminaliteit, meer cybercrime.* https://www.cbs. nl/nl- nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime
CBS. (2020b, 2 maart). *Veiligheidsmonitor 2019*. https://www.cbs.nl/nl- nl/publica tie/2020/10/veiligheidsmonitor-2019
Ceesay, E., Myers, K., & Watters, P. (2018). Human-centred strategies for cyber-physical se curity. *EAI Endorsed Transactions on Security and Safety, 18*(4), e5. https://doi. org/10.4108/eai.15-5- 2018.154773
Christofides, E., & Muise, A. (2012). Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior. *Journal of Adolescent Research, 27*(6), 714–731. https://doi.org/10.1177/0743558411432635
Cleiren, C. P. M., Ten Voorde, J. M., & Waas, W. V. (2019). Strafbaarstelling van sexchatting en sextortion onder de loep. De meerwaarde van een empirisch perspectief. *Strafblad, 2*, 69-76.
Debatin, B. Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108. https://doi.org/10.1111/j.1083-6101.2009.01494.x
Dehghanniri, H., & Borrion, H. (2019). Crime scripting: A systematic review. *European Jour nal of Criminology*. https://doi.org/10.1177/1477370819850943
Dodge, A. (2016). Digitizing rape culture: Online sexual violence and the power of the digital photograph. *Crime, Media, Culture, 12*(1), 65-82. https://doi. org/10.1177/1741659015601173
Domenie, M. M. L., Leukfeldt, E. R., van Wilsem, J, A., Jansen, J., & Stol, W. P. (2013). *Slachtof ferschap in een gedigitaliseerde samenleving.* Boom Lemma Uitgevers.
Eurostat (2018). *Households – level of Internet access.* http://appsso.eurostat.ec.europa.eu/ nui/show.do?dataset=isoc_ci_in_h&lang=en;
Frieze, S. (2014) *Qualitative data analysis with ATLAS.ti.* New York : SAGE.
Geng, G. G., Lee, X. D., & Zhang, Y. M. (2014). Combating Phishing Attacks via Brand Identity and Authorization Features. *Security and Communication Networks, 8*(6), 888–898. https://doi.org/10.1002/sec.1045

Gercke, M. (2007). *Internet-related identity theft*. Council of Europe. https://www.combattingcybercrime.org/files/virtual-library/phenomena-challenges-cybercrime/internet-related-identity-theft%E2%80%93a-discussion-paper.pdf
Holt, T. J. & Turner, M. G. (2012). Examining Risks and Protective Factors of On-Line Identity Theft. *Deviant Behavior, 33*(4), 308-323. https://doi.org/10.1080/01639625.2011.584050.
Holt, T. J., & Bossler A. M. (2013). Examining the Relationship Between Routine Activities and Malware Infection Indicators. *Journal of Contemporary Criminal Justice, 29*(4), 420-436. https://doi.org/10.1177/1043986213507401
Holt, T. J., Bossler, A. M., Malinski, R., & May, D. C. (2016). Identifying predictors of unwan ted online sexual conversations among youth using a low self-control and routine activity framework. *Journal of Contemporary Criminal Justice, 32*(2), 108-128. https:// doi.org/10.1177/1043986215621376
Holt, T. J. Weijer, S. Leukfeldt, R. Wilsem, J. (2020). Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization. *Social Science Computer Review, 38*(2), 187–206. https://doi.org/10.1177/0894439318805067
Jansen, J. (2018). Do you bend or break? *Preventing online banking fraud victimization through online resilience* [Doctoral thesis, Open Universiteit]. https://research. ou.nl/ws/portalfiles/portal/9260429/2018_Proefschrift_Jansen.pdf
Jansen, J., Leukfeldt, E. R., van Wilsem, J., & Stol, W. (2013). Een risico voor hacken en per soonsgerichte cyberdelicten?. *Tijdschrift voor Criminologie,* 55, 4.
Jong, L., Leukfeldt, E. R., & van de Weijer, S. (2018). Determinanten en motivaties voor in tentie tot aangifte na slachtofferschap van cybercrime. *Tijdschrift voor Veiligheid,* 2018(1-2), 66-78. https://doi.org/ 10.5553/tvv/187279482018017102006
Kievik, M., Misana-ter Huurne, E. F. J., Gutteling, J. M., & Giebels, E. (2018). Making it stick: Exploring the effects of information and behavioral training on self-protectiveness of citizens in a real- life safety *setting. Safety Science*, 101, 1-10. https://doi.org/10.1016/j.ssci.2017.08.007
Kleve, P., De Mulder, R., & Van Noortwijk, K. (2011). The definition of ICT Crime. *Computer Law & Security Review, 27*(2), 162-167.
Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551-555. https://doi.org/10.1089/cyber.2014.0008
Leukfeldt, E. R. (2015). Comparing victims of phishing and malware attacks: Unraveling risk factors and possibilities for situational crime prevention. *International Journal of Advanced Studies in Computer Science and Engineering, 4*(5), 26-32.
Leukfeldt, E. R., Kentgens, A., Prins, E., & Stol, W. (2015). Alledaags politiewerk in een gedigitaliseerde wereld. Handreiking voor de intake van delicten met een digitale component. Lectoraat Cybersafety (NHL Hogeschool/Politieacademie)/ Open Universiteit.

Leukfeldt, E. R., Spithoven, R. & Misana-ter Huurne, E. F. J. (2020). De lokale aanpak van cybercrime. Risicocommunicatie als antwoord op een grenzeloos vraagstuk. In C. de Poot et al. (Eds.), *Politie en cybercriminaliteit* (pp. 203-222). Gompel&Scavina.

Leukfeldt, E. R. Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior,* 37(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Leukfeldt, E. R., Notte, R., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na*. WODC & NSCR. https://repository.wodc.nl/handle/20.500.12832/2355

Leukfeldt, E. R., Notte, R., & Malsch, M. (2019). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. *Victims and Offenders*, 15(1), 60-77. https://doi.org/10.1080/15564886.2019.1672229.

Misana-ter Huurne, E., Van Houten, Y., Spithoven, R., Notté, R., & Leukfeldt, R. (2020, februari). *Cyberweerbaarheid: risicobewustzijn en zelfbeschermend gedrag rond om cybercriminaliteit onder jongeren en mkb-ers.* Saxion. https://www.saxion.nl/binaries/content/assets/onderzoek/areas--living/maatschappelijke- veiligheid/saxion--haagse-hogeschool---cyberweerbaarheid.-risicobewustzijn-en- zelfbescher mend-gedrag-rondom-cybercrime-onder-jongeren-en-mkb-ers..pdf

Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race. Over cyberdreigingen en versterking van weerbaarheid.* Rathenau Instituut. https://www.rathenau.nl/nl/digitale- samenleving/een-nooit-gelopen-race

Nationaal Cyber Security Centrum (NCSC). (2016, 5 september). *Cybersecuritybeeld Nederland 2016*. Nationaal Cöordinator Terrorismebestrijding en Veiligheid. https://www.nctv.nl/onderwerpen/cybersecuritybeeld- nederland/documenten/publicaties/2016/09/05/cybersecuritybeeld-nederland-2016

Nederlandse Vereniging van Banken. (2020, 16 april). *Veel meer phishing en bankpasfraude in 2019*. https://www.nvb.nl/nieuws/veel-meer-phishing-en-bankpasfraude-in-2019/

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: an examination of individual and situational level factors. *International Jouranal of Cyber Criminology,* 5(1), 773-793.

Paulissen, L., & Wilsem, J. (2015). *Dat heeft iemand anders gedaan! Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland*. Politie en Wetenschap. https://www.politieenwetenschap.nl/publicatie/politiewetenschap/2015/dat-heeft-iemand- anders-gedaan-259/

Patchin, J. W., & Hinduja, S. (2020). Sextortion among adolescents: results from a national survey of US youth. Sexual Abuse, 32(1), 30-54. https://doi.org/10.1177/1079063218800469

Politie (2020a). *Meer misdrijven in 2019,* daders steeds jonger. https://www.politie.nl/nieuws/2020/januari/15/cijfers.html

Politie (2020b). *Geregistreerde misdrijven en aangiften; soort misdrijf, gemeente.* https://data.politie.nl/#/Politie/nl/dataset/47013NED/table?ts=1602081258997

Powell, A., Nicola, H., Asher, F., & Scott, A. J. (2019). Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian residents. *Computers in Human Behavior*, 92, 393-402. https://doi.org/10.1016/j.chb.2018.11.009.

Renes, R. J., van den Putte, B., van Breukelen, R., Loef, J., Otte, M., & Wennekers, C. (2011). *Gedragsverandering via campagnes. Literatuuronderzoek in opdracht van Dienst Publiek en Communicatie.* Ministerie van Algemene Zaken. https://edepot.wur.nl/182073

Roelofs, M., de Koning, N.M., van Vliet, A. J., Wijn, R., van Rijk, R., & Young, H. J. (2018). *De menselijke kant van cybersecurity: Conceptuele ontwikkelingen en de Cyber Securi ty Assistent*. TNO.

Saldaña, J. (2012) *The Coding Manual for Qualitative Researchers.* Second edition. London : SAGE Publications.

Schulz, A., Bergen, E., & Schuhmann, P. (2016). Online Sexual Solicitation of Minors: How Often and between Whom Does It Occur? *Journal of Research in Crime and Delinquency,* 53(2), 165- 188. https://doi.org/10.1177/0022427815599426

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382.

Simms, C. (2016). A matter of survival. *ITNow*, 58(4), 30-31. doi:10.1093/itnow/bww102.

Sipma, T., & van Leijsen, E. M. C. (2019). *Slachtofferschap van online criminaliteit: Prevalentie, risicofactoren en gevolgen.* WODC. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/11/28/tk- bijlage-slachtofferschap-van-online-criminaliteit/tk-bijlage-slachtofferschap-van-online- criminaliteit.pdf

Spithoven, R. (2020). *Verbonden risico's. Maatschappelijke veiligheid in de black box society*. Den Haag: Boom Criminologie.

Sweeney, L. & Ruth, S. (2006). Protecting job seekers from identity theft. *IEEE Internet Computing, 10*(2), 74-78. https://doi.org/10.1109/MIC.2006.40

Talib, S. Clarke, N. Furnell, S. (2010). An Analysis of Information Security Awareness within Home and Work Environments. *2010 International Conference on Availability, Reliability and Security,* 196-203. https://doi.org/10.1109/ares.2010.27

Ter Huurne, E. F. J. (2008). I*nformation seeking in a risky world : the theoretical and empirical development of FRIS : a Framework of Risk Information Seeking* [Doctoral thesis, University of Twente].

Tollenaar, N., Rokven, J., Macro, D., Beerthuizen, M., & van der Laan, A. M. (2019). *Predictieve textmining in politieregistraties*. WODC. https://repository.wodc.nl/handle/20.500.12832/220

Van de Weijer, S. G., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking, 20*(7), 407-412. https://doi.org/10.1089/cyber.2017.0028

Van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal, 43*(1), 17-34. https://doi.org/10.1108/PIJPSM-07-2019-0122

Van der Grient, R., Schippers, N., & Hengstz, K. (2020, 1 oktober). *Veilig Online 2020*. Ministerie van Economische Zaken en Klimaat & Motivaction. https://www.rijksoverheid.nl/documenten/rapporten/2020/09/30/veilig-online-2020

Van der Kleij, R., De Bruin, I., Van 't Hoff–de Goede, S. & Leukfeldt, R. (2019, 7 maart). *Pilotonderzoek cyberweerbaarheid MKB-retailers in de regio Den Haag.* De Haagse Hogeschool. https://www.dehaagsehogeschool.nl/docs/default-source/documenten- onderzoek/lectoraten/cybersecurity-in-het-mkb/cyberweerbaarheid-mkb- retailers.pdf?sfvrsn=49327266_0

Van 't Hoff-de Goede, S., van der Kleij, R., van de Weijer, S., & Leukfeldt, E. R. (2019). *Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders*. WODC, Centre of Expertise Cybersecurity (Haagse Hogeschool) & NSCR. https://repository.wodc.nl/handle/20.500.12832/2433

Van 't Hoff-de Goede, S., Leukfeldt, R., Van der Kleij, R., & Van de Weijer, S. (2021). The Online Behaviour and Victimization Study: the development of an experimental research instrument for measuring and explaining online behaviour and cybercrime victimization. In M. Weulen Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in Context* (in print).

Van Wilsem, J. (2013). 'Bought it, but never got it': Assessing risk factors for online consumer fraud. *European Sociological Review, 29*(2), 168-178. https://doi.org/10.1093/esr/jcr053

Veenstra, S., Zuurveen, R., & Stol, W. (2015, mei). *Cybercrime onder bedrijven: Een onderzoek naar slachtofferschap van cybercrime onder het midden-en kleinbedrijf en zelfstandigen zonder personeel in Nederland.* Cybersafety Research Group. https://cybersciencecenter.nl/media/1054/2015-05-13-cybercrime-onder-bedrijven-def.pdf

Walker, K., & Sleath, E. (2017). A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. *Aggression and Violent Behavior*, 36, 9-24. https://doi.org/10.1016/j.avb.2017.06.010

Wade, C. R., Molony, S. T., Durbin, M. E., Klein, S. H., & Wahl, L. E. (1992, september). *Communicating with the Public about Risk*. U.S. Department of Energy. https://www.osti.gov/servlets/purl/7238850

Williams, M. L. (2016). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *British Journal of Criminology, 56*(1), 21-48. https://doi.org/10.1093/bjc/azv011

Wolak, J., & Finkelhor, D. (2016, juni). *Sextortion: Findings from a survey of 1,631 victims.* Crimes Against Children Research Center. https://www.wearethorn.org/wp-content/uploads/2016/08/Sextortion_Report.pdf

Worsley, J. D., Jacqueline, M., & Short, E. (2017). Victims' voices: Understanding the emotional impact of cyberstalking and individuals' coping responses. *SAGE Open*, 7(2). doi:10.1177/2158244017710292

Bijlage 1: Het Cyber Resilience Model

Het Cyber Resilience Model is gebaseerd op kennis over zelfbeschermend gedrag ten aanzien van (veiligheids)risico's in de offline wereld en voegt relevante elementen samen uit bestaande theorieën en modellen, waaronder de Protectie Motivatie Theorie (Rogers, 1983), de Theory of Planned Behavior (Ajzen, 1991), het Framework of Risk Information Seeking (ter Huurne, 2008) en aanpalende inzichten uit de risicoperceptie en criminologische literatuur. Hieronder volgt een beschrijving van de elementen in het model.

Onder **zelfbeschermend gedrag** verstaan wij: die acties of gedragingen die mensen uitvoeren om zichzelf te beschermen tegen risico's, gevaren of de gevolgen daarvan (inclusief negatieve emoties). In de basis kunnen mensen op twee manieren reageren op mogelijke risico's: problem- focused coping of emotion-focused coping. De intentie om dit gedrag uit te voeren is een belangrijke voorspeller van het daadwerkelijk gedrag (Ajzen, 1991).

Target hardening is het gedrag dat beoogd wordt te bereiken door middel van risicocommunicatie campagnes: mensen gaan hun gedrag aanpassen op basis van de gegeven gedragsadviezen met als doel zichzelf te beschermen tegen het gevaar. Toegepast op de risico's van cybercriminaliteit kan dit op verschillende manieren:

(I) Door fysieke maatregelen te treffen (wachtwoorden instellen, anti-phishing software, etc.)
(II) Door gedragsmatige maatregelen (informatie zoeken, alertheid, bewustzijn, veilig handelen)

De **gedragsintentie** om preventief gedrag ten aanzien van cybercriminaliteit te nemen komt tot stand langs verschillende factoren:

(I) de perceptie van het risico; Onder **risicoperceptie** verstaan wij de wijze waarop een individu het risico voor hem inschat, is afhankelijk van verschillende factoren. Ten eerste moet er een **dreiging** ervaren worden. Deze dreiging bestaat uit de inschatting van de kans dat de persoon blootgesteld wordt aan een risico en de ingeschatte **ernst** van de mogelijke effecten. Dit zijn de mate van **risicogevoeligheid, kwetsbaarheid en slachtofferschap**. Het hebben van ervaring, kennis en bewustzijn van de aanwezigheid van het risico of gevaar speelt hierbij een belangrijke rol. Zo is aandacht voor het risico in de **sociale omgeving** (een kennis is slachtoffer geworden van phishing of malware) of in de **media** een belangrijke trigger van risicoperceptie. De **kennis** die een persoon daardoor opdoet over het risico, beïnvloedt het risicobewustzijn. De mate waarin de persoon zich bewust is van zijn mogelijke persoonlijke risico door deze aandacht is van invloed op de risicoperceptie.

(II) de beleving van ofwel de **affectieve respons** op het risico. Risicoperceptie is niet alleen een puur cognitieve inschatting van het gevaar of het risico. Door kennis, informatie, (sociale of media) aandacht en bewustzijn, ontstaat er vaak een affectieve respons. Deze respons is voornamelijk gebaseerd op emoties, intuïtie en onderbuikgevoel en is vaak een onbewuste reactie (Lindell & Perry, 2012). Deze reactie is echter van grote invloed op de **risicobeleving** en het uiteindelijke gedrag van mensen (Slovic, 2004; Finucane e.a., 2000).

Onder **'behavioural beliefs'** verstaan wij de mate waarin men zichzelf in staat acht het gedrag echt te kunnen uitvoeren en in hoeverre het uitvoeren van dit gedrag bijdraagt aan het minimaliseren van het gevaar of de mogelijke gevolgen daarvan. Hierbij zijn vier inschattingsstadia aanwezig:

(I) Inschatting eigen kwetsbaarheid ten opzichte van het gevaar;
(II) Inschatting van de ernst van de dreiging en gevolgen daarvan;
(III) Inschatting van de effectiviteit van het aanbevolen gedrag;
(IV) Inschatting van de eigen effectiviteit (de mate waarin een persoon zichzelf in staat acht het aanbevolen gedrag uit te kunnen voeren).

Stadia 1 en 2 vormen samen de **risicoperceptie.** Stadia 3 en 4 vormen samen de **effectiviteitsverwachting.**

De gedragsintentie wordt tevens beïnvloed door **subjectieve normen** - de sociale aanmoediging van gedrag en geldende normen in de omgang met het risico van cybercriminaliteit. Gegeven de complexiteit van dit proces is het zaak om per doelgroep - op maat - in te spelen op deze samenhangende concepten om effect te sorteren en doelgroepen - in plaats van naar passieve (A) emotion focused coping onder invloed van psychologische beschermingsmechanismen – naar actieve (B) target hardening te brengen en zo hun cyberweerbaarheid te vergroten.

Bijlage 2: Interviewvragen gemeenten

Beste [naam],

Allereerst hartelijk dank dat u wilt meewerken aan dit onderzoek.
Dit interview gaat over cybercrime en is onderdeel van het onderzoek dat Hogeschool Saxion en de Haagse Hogeschool in samenwerking met u als consortiumpartner uitvoeren om te komen tot effectieve interventies voor ambtenaren openbare orde en veiligheid om de cyberweerbaarheid binnen hun gemeente te vergroten. [zo nodig extra informatie over het project geven, afhankelijk van voorkennis geïnterviewde]

Dit gesprek richt zich op het inzichtelijk krijgen van de mogelijke doelgroepen en typen cybercrime die gemeentes belangrijk achten om daar in het kader van preventie iets mee te gaan doen. Ook willen we inzicht krijgen in de activiteiten die u op het gebied van cyberweerbaarheid al doet of gaat doen, en in hoe u uw rol ziet in het vergroten van de cyberweerbaarheid onder inwoners en mkb'ers.
Omdat wij meerdere personen interviewen, worden geluidsopnames gemaakt van dit gesprek. Deze opnames worden alleen gebruikt voor de analyse van uw interview. Alles wat u zegt of vindt, zal geanonimiseerd worden verwerkt en uw antwoorden zullen op geen enkele wijze met u als persoon in verband kunnen worden gebracht. Na analyse worden deze opnames vernietigd. Uw anonimiteit is volledig gewaarborgd.

Er zijn geen goede of foute antwoorden, uw mening en ideeën staan centraal.

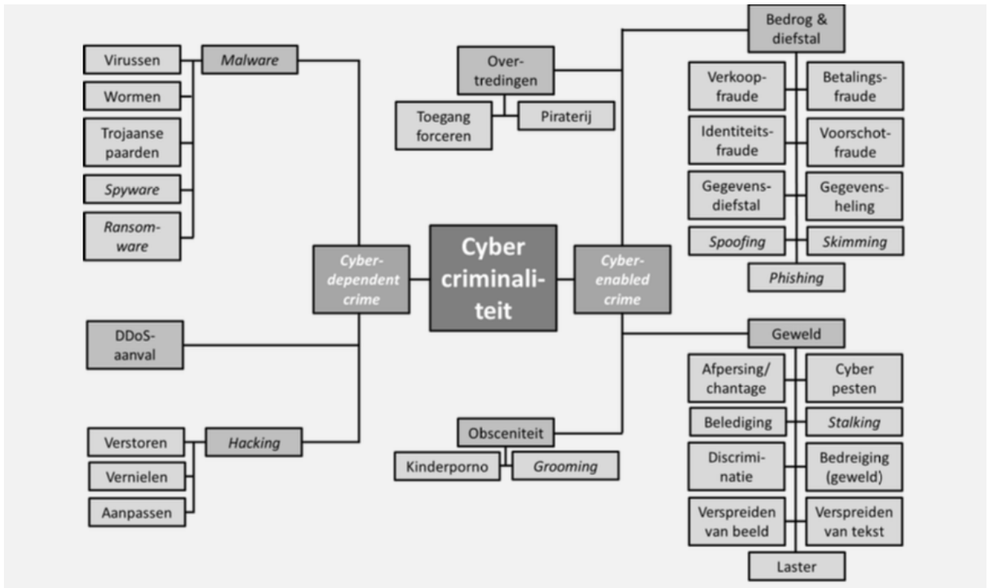
Als u verder geen vragen heeft, dan stel ik voor dat we gaan beginnen.

1. Bij welke gemeente werkt u en wat is uw functie daar?

2. Wat verstaat u onder cybercriminaliteit?*

3. Welke raakvlakken heeft uw werk met cybercriminaliteit?

* **Neem de definitie van (I) cybercriminaliteit en (II) de taxonomie van cybercriminaliteit door om op een lijn te komen**
I. Definitie cybercriminaliteit
(Spithoven 2020,. op basis van Kleve, De Mulder & Van Noortwijk, 2010; Holt & Bossler, 2013; Leukfeldt, 2016, 2018; Holt, Bossler & Seigfried-Spellar, 2018)
Cyber-criminaliteit betreft het gebruiken van het internet of andere computertechnologie ten behoeve van het faciliteren van criminaliteit of ander normoverschrijdend gedrag.
Onder (I) *cyber-enabled criminaliteit* worden klassieke vormen van criminaliteit verstaan, die door middel van ICT op een grotere schaal kunnen worden uitgevoerd, zoals oplichting, identiteitsfraude en *phishing*.
Onder (II) *cyber-dependent criminaliteit*wordt criminaliteit verstaan die wordt gepleegd door middel van ICT met ICT als doelwit, zoals hacks, DDoS-aanvallen, virussen, ransomware en andere malware.



II. Taxonomie cybercriminaliteit (Spithoven 2020, p. 49)

4. Welke doelgroepen worden er volgens u vooral het slachtoffer van cybercriminaliteit?

a. Waarop baseert u deze doelgroepen? Waarom deze doelgroepen?
b. Worden ergens cijfers geregistreerd binnen uw gemeente over slachtofferschap?
c. Via welke partijen komt u aan cijfers of inschattingen van slachtofferschap van cybercriminaliteit?
d. Krijgen jullie momenteel dergelijke cijfers of informatie van de politie? Zo ja: wat voor cijfers of informatie? Loopt dit goed of moet dit anders?
e. Hebben jullie ook cijfers of informatie over slachtofferschap beschikbaar van an dere partijen dan de politie? Zo ja: Welke partijen? Wat voor cijfers of infor matie? Loopt
dit goed of moet dit anders?
f. Welke cijfers of informatie zouden jullie nodig hebben om een goede inschatting te maken van slachtofferschap van cybercriminaliteit? Welke partijen spelen daarbij een rol?
g. Heeft u zicht op dergelijke cijfers en wat de cijfers zijn voor verschillende typen cybercrime?
h. Van welke typen cybercrime worden de benoemde doelgroepen slachtoffer? Zijn er typen cybercrime die opvallend vaak gemeld worden? Waarom is dat denkt u?
i. Hoe zijn deze typen cybercrime verdeeld over de doelgroepen? Is er een lijn in te ontdekken?

5. Wat zijn volgens u de belangrijkste oorzaken voor slachtofferschap van cybercriminaliteit onder burgers en ondernemers?

a. Waarop baseert u deze oorzaken?
b. Zijn deze oorzaken voor u momenteel duidelijk of juist vaag?

6. Wat verstaat u onder cyberweerbaarheid (eventueel refereren naar titel van ons project)?*

*III. Definitie cyberweerbaarheid (Spithoven, 2020; Misana-ter Huurne e.a., 2020)
De combinatie van een voldoende hoge mate van risicobewustzijn en zelfbeschermend gedrag onder burgers en ondernemers om slachtofferschap van cybercriminaliteit te voorkomen en/of mogelijke impact te voorkomen of verkleinen.

7. Voor welke doelgroepen is het vergroten van de cyberweerbaarheid volgens u het meest noodzakelijk? Waarom?
8. Voor welke typen cybercrime is het vergroten van de cyberweerbaarheid van deze doel groepen volgens u het meest noodzakelijk? Waarom?

Professionele inschattingen

9. Waar liggen volgens u de juridische en maatschappelijke taken en verantwoorde lijkheden van een gemeente in de bestrijding van cybercrime?

Beleidsmatige opvattingen en praktische aanpak

10. Volgens u, moet de gemeente verder gaan dan deze verantwoordelijkheden en zich bezighouden met bevorderen van cyberweerbaarheid onder burgers en ondernemers?
11. In een ideale wereld, hoe zouden deze taken volgens u het meest effectief en efficiënt in de
gemeente ingebed moeten worden?
12. Zijn er binnen uw organisatie voorgenomen werkzaamheden ter bevordering van de cyberweerbaarheid onder burgers en ondernemers?
a. Zijn deze werkzaamheden op beleid gebaseerd?
b. Hoe is dit beleid tot stand gekomen? Werkt u hierin samen met partners? Structureel en/of projectmatig? Met wie? En waarom?
c. Heeft dit beleid prioriteit binnen uw organisatie? Waarom wel/niet?
d. Welke resultaten verwacht u op welke wijze te behalen? Hoe worden deze doelstellingen concreet in de praktijk uitgewerkt?
13. Wordt dit beleid ook geëvalueerd?
a. Wat waren de resultaten van eventuele eerdere evaluaties?

Best practices

14. Zijn er in uw organisatie ‘best practices’ ontwikkeld ter bevordering van de cyberweerbaarheid van burgers en ondernemers? (best practice: een manier van werken waarbij is bewezen dat deze manier de meest efficiënte en effec tieve manier is om tot het gewenste resultaat of doelstelling te komen)
a. Hoe zijn deze tot stand gekomen?
b. Hoe hebben deze ‘best practices’ zich bewezen?
c. Heeft u deze ‘best practices’ ook met andere professionals gedeeld?
d. Hoe verhouden deze ‘best practices’ zich met de doelgroepen die slachtof fer worden van cybercrime?

Uitdagingen

15. Zijn er zaken die uw werkzaamheden om de cyberweerbaarheid van burgers en ondernemers te bevorderen ingewikkeld maken of belemmeren? En voor gemeenten in het algemeen?
a. Wat zijn mogelijke oplossingsrichtingen voor deze zaken?

Ondersteuningsbehoefte

16. Heeft u behoefte aan ondersteuning bij het bevorderen van de cyberweerbaar heid van burgers en ondernemers?
a. Welke ondersteuning zou u willen hebben en van wie?

Afsluiting

17. Welke kansen/verbeteringen om de cyberweerbaarheid van burgers en onderne mers te vergroten ziet u voor de toekomst?

18. Hebben wij in dit interview nog iets gemist dat u wilt meegeven?

19. Met wie moeten wij volgens u nog spreken? -> interviews met experts over cyber crime

Hartelijk dank voor uw medewerking. Wellicht tot ziens bij een volgende consortiumbijeenkomst.

Bijlage 3: Interviewvragen experts

Beste [naam],

Allereerst hartelijk dank dat u wilt meewerken aan dit onderzoek.

Dit interview gaat over cybercrime en is onderdeel van het onderzoek dat Hogeschool Saxion en de Haagse Hogeschool in samenwerking met gemeenten en regionale veiligheidsnetwerken uitvoeren om te komen tot effectieve interventies voor ambtenaren openbare orde en veiligheid om de cyberweerbaarheid binnen hun gemeente te vergroten. [zo nodig extra informatie over het project geven, afhankelijk van voorkennis geïnterviewde]
Een eerste stap in het project is het verkrijgen van inzicht in de mogelijke doelgroepen en typen cybercrime om daar in het kader van preventie iets mee te gaan doen. Naast een literatuurstudie en praktijkinzichten van lokale overheden, vinden wij het belangrijk om ook de mening en visie van experts uit het brede werkveld van cybercrime mee te nemen. Op basis van uw kennis en expertise hebben we u daarom gevraagd voor dit gesprek.
Omdat wij meerdere personen interviewen, worden geluidsopnames gemaakt van dit gesprek. Deze opnames worden alleen gebruikt voor de analyse van uw interview. Alles wat u zegt of vindt, zal geanonimiseerd worden verwerkt en uw antwoorden zullen op geen enkele wijze met u als persoon in verband kunnen worden gebracht. Na analyse worden deze opnames vernietigd. Uw anonimiteit is volledig gewaarborgd.

Er zijn geen goede of foute antwoorden, uw mening en ideeën staan centraal.

Als u verder geen vragen heeft, dan stel ik voor dat we gaan beginnen.

We starten met drie vragen over u en uw functie.
1. Bij welke organisatie werkt u en wat is uw functie daar?
2. Welke raakvlakken heeft uw werk met cybercriminaliteit?
3. Wat is uw expertise op het gebied van cybercriminaliteit?

Tijdens dit gesprek zou ik graag met u over cybercriminaliteit willen spreken. Wij hanteren voor cybercriminaliteit de brede definitie, waaronder zowel cyber-enabled criminaliteit als cyber- dependent criminaliteit valt. Onder cyber-enabled criminaliteit vallen klassieke vormen van criminaliteit, die door middel van ICT op een grotere schaal kunnen worden uitgevoerd, zoals oplichting, identiteitsfraude en phishing. Onder cyber-dependent criminaliteit wordt criminaliteit verstaan die wordt gepleegd door middel van ICT met ICT als doelwit, zoals hacks, DDoS-aanvallen, virussen, ransomware en andere malware.

Dan zou ik het nu graag willen hebben over de meest voorkomende delicten en slachtoffers.

4.
- a. Welke typen cybercriminaliteit komen volgens u het meest voor?
- b. Waarop baseert u dit? Hoe weet u dit?
- c. Maakt u hierbij gebruik van cijfers over slachtofferschap van cybercrimina liteit? Wat voor cijfers? Via welke partijen komt u aan deze cijfers?

5.
- a. Welke mensen/groepen worden er volgens u vooral het slachtoffer van cybercriminaliteit?
- b. Waarop baseert u deze slachtoffers? En hoe accuraat is volgens u deze inschatting?
- c. Maakt u hierbij gebruik van cijfers over slachtofferschap van cybercrimina liteit? Wat voor cijfers? Via welke partijen komt u aan deze cijfers?
- d. Registreert jullie organisatie zelf ook cijfers van slachtofferschap van cybercriminaliteit?

6. Uit een eerste interviewronde met gemeenten en een literatuurstudie komt naar voren, dat bepaalde cyberdelicten en slachtoffergroepen het meest voor lijken te komen. Kunt u voor de volgende delicten en slachtoffergroepen aangeven of u dit herkent?

hier doorvragen op het evt. verschil met de antwoorden die respondent bij de vragen 1 en 2 heeft gegeven.

Delicten
- a. Hacking
- b. Koop- en verkoopfraude
- c. Identiteitsfraude
- d. Malware
- e. Phishing
- f. interpersoonlijke incidenten met een seksuele (bij)bedoeling

Groepen
- g. Jongeren
- h. Ouderen
- i. Mkb

Dan zou ik het nu graag willen hebben over de verklaringen van slachtofferschap van cybercriminaliteit en hoe slachtofferschap kan worden voorkomen.

7.
- a. Wat zijn volgens u de belangrijkste oorzaken voor slachtofferschap van cybercriminaliteit?
- b. Waarop baseert u deze oorzaken? Hoe weet u dat?
- c. Verschillen deze oorzaken voor de genoemde doelgroepen?

Ik wil u graag iets vertellen over de term cyberweerbaarheid die centraal staat in ons onderzoek. De mens wordt geregeld omschreven als de zwakste schakel in cybersecurity en een manier om slachtofferschap van cybercriminaliteit terug te dringen is het verbeteren van de cyberweerbaarheid van internetgebruikers.
Onder cyberweerbaarheid verstaan wij daarbij de combinatie van een voldoende hoge mate van risicobewustzijn en zelfbeschermend gedrag onder burgers en ondernemers om slachtofferschap van cybercriminaliteit te voorkomen en/of mogelijke impact te voorkomen of verkleinen.
Ons project richt zich op het vergroten van de cyberweerbaarheid en zelfbeschermend gedrag van burgers en ondernemers en interventies die gemeenten hierbij kunnen inzetten.

8. Wat vindt u ervan dat dit project zich richt op het verbeteren van cyberweerbaarheid ?

9.
- a. Heeft u in uw werkzaamheden/ uw organisatie ook aandacht voor het bevorderen van de cyberweerbaarheid van burgers en ondernemers?
- b. Zo ja, wat doet u precies?
- c. Waarop richt zich dat specifiek / hoe draagt dat bij aan de cyberweerbaarheid?
- d. Hoe effectief is dat?

10. Voor welke doelgroepen is het vergroten van de cyberweerbaarheid volgens u het meest noodzakelijk? Waarom?

11. Voor welke typen cybercrime is het vergroten van de cyberweerbaarheid van elk van deze doelgroepen volgens u het meest noodzakelijk? Waarom?

Dan zou ik het nu graag willen hebben over trends en verwachtingen voor de toekomst met betrekking tot cybercriminaliteit en slachtofferschap.

12.
- a. Voorziet u in de komende jaren andere/aanvullende doelgroepen voor wie het vergroten van de cyberweerbaarheid noodzakelijk is?
- b. Zo ja, welke en waarom?

13.
- a. Voorziet u in de komende jaren nieuwe typen cybercrime waartegen het vergroten van de cyberweerbaarheid in de komende jaren noodzakelijk is?
- b. Zo ja, welke en waarom?
- c. Voorziet u daarbij ook relevante ontwikkelingen in de werkwijzen van criminelen?

Afsluiting

14. Hebben wij in dit interview nog iets gemist dat u wilt meegeven? Bijlage 4: Vragenlijst toetsing eerste resultaten aan inzichten praktijkpartners
MKB vragenlijst

Bijlage 4: Vragenlijst toetsing eerste resultaten aan inzichten praktijk-partners

MKB vragenlijst

Doel

- verifiëren van de uitkomsten van het lopende onderzoek bij lokale partijen. Klopt het beeld per doelgroep (jongeren, ouderen, mkb'ers) voor wat betreft de cyberdelicten waar zij slachtoffer van worden?
- Het vaststellen van de do's en don'ts bij het aanspreken of bereiken van de doelgroep

Algemene info:

- Naam organisatie + functie gesprekspartner:_____
- Relatie tot de doelgroep:_____

1. MALWARE

1. Herken jij dat deze mkb'ers slachtoffer worden van malware?
2. Hoe komt het volgens jou dat in deze doelgroep slachtoffers vallen? Wat zijn volgens jou kenmerkende eigenschappen of gedragingen?
3. Wat is de schade die slachtoffers oplopen en hoe groot is de impact van slachtofferschap volgens jou?
4. Op welke manier zoeken slachtoffers hulp? Weten ze waar ze terecht kunnen en waar hebben zij behoefte aan?
5. We willen bij mkb'ers bereiken dat ze zich beter gaan beschermen tegen malware, door zowel technische voorzorgsmaatregelen te treffen, als het uitvoeren van zelfbescher mend gedrag.
    a. Als we dit willen bereiken, waar moeten we dan volgens jou rekening mee houden bij het ontwikkelen van een interventie?
    b. Wat zijn volgens jou goede manieren om deze groep te benaderen?
    c. Op welke wijze kan het gedrag van leden van de groep goed beïnvloed wor den?
    d. Waar zijn zij wel/ niet vatbaar voor?

2. HACKING

1. Herken jij dat mkb'ers slachtoffer worden van hacking?

2. Hoe komt het volgens jou dat in deze doelgroep slachtoffers vallen? Wat zijn vol gens jou kenmerkende eigenschappen of gedragingen? 83
3. Wat is de schade die slachtoffers oplopen en hoe groot is de impact van slachtof ferschap volgens jou?
4. Op welke manier zoeken slachtoffers hulp? Weten ze waar ze terecht kunnen en waar hebben zij behoefte aan?
5. We willen bij mkb'ers bereiken dat ze zich bewust zijn van de risico's van hacking en dat ze zich beter gaan beschermen, zowel door technische maatregelen als zelfbeschermend gedrag.
    a. Als we dit willen bereiken, waar moeten we dan volgens jou rekening mee houden bij het ontwikkelen van een interventie?
    b. Wat zijn volgens jou goede manieren om deze groep te benaderen?
    c. Op welke wijze kan het gedrag van leden van de groep goed beïnvloed wor den?
    d. Waar zijn zij wel/ niet vatbaar voor?

3. PHISHING

1. Herken jij dat mkb'ers slachtoffer worden van phishing?
2. Hoe komt het volgens jou dat ouderen hier slachtoffer van worden? Wat zijn vol gens jou kenmerkende eigenschappen of gedragingen?
3. Wat is de schade en de impact hiervan volgens jou voor de slachtoffers?
4. Op welke manier zoeken slachtoffers hulp? Weten ze waar ze terecht kunnen en waar is behoefte aan?
5. We willen bij mkb'ers bereiken dat ze zich beter informeren over en beschermen tegen phishing, door hun gedrag aan te passen, alerter te zijn en technische maatregelen treffen.
    a. Als we dit willen bereiken, waar moeten we dan volgens jou rekening mee houden bij het ontwikkelen van een interventie?
    b. Wat zijn volgens jou goede manieren om deze groep te bereiken?
    c. Op welke wijze kan het gedrag van deze groep goed beïnvloed worden?
    d. Waar zijn zij wel/niet vatbaar voor?

Ouderen vragenlijst

Doel

- verifiëren van de uitkomsten van het lopende onderzoek bij lokale partijen. Klopt het beeld per doelgroep (jongeren, ouderen, mkb'ers) voor wat betreft de cyberdelicten waar zij slachtoffer van worden?
- Het vaststellen van de do's en don'ts bij het aanspreken of bereiken van de doelgroep

Algemene info:
- Naam organisatie + functie gesprekspartner:_____
- Relatie tot de doelgroep:_____

1. VRIEND-IN-NOOD-FRAUDE (Whatsapp-fraude)

6. Herken jij dat deze doelgroep slachtoffer wordt van vriend-in-nood-fraude?
7. Hoe komt het volgens jou dat in deze doelgroep slachtoffers vallen? Wat zijn volgens jou kenmerkende eigenschappen of gedragingen?
8. Wat is de schade die slachtoffers oplopen en hoe groot is de impact van slachtofferschap volgens jou?
9. Op welke manier zoeken slachtoffers hulp? Weten ze waar ze terecht kunnen en waar hebben zij behoefte aan?
10. We willen bij ouderen bereiken dat ze zich bewust zijn van de risico's van vriend-in-nood-fraude, weten hoe ze slachtoffer kunnen worden en voorkomen en dat ze alerter worden op verdachte situaties.
    a. Als we dit willen bereiken, waar moeten we dan volgens jou rekening mee houden bij het ontwikkelen van een interventie?
    b. Wat zijn volgens jou goede manieren om deze groep te benaderen?
    c. Op welke wijze kan het gedrag van leden van de groep goed beïnvloed worden?
    d. Waar zijn zij wel/ niet vatbaar voor?

2. HELPDESKFRAUDE

6. Herken jij dat ouderen slachtoffer worden van helpdeskfraude?
7. Hoe komt het volgens jou dat in deze doelgroep slachtoffers vallen? Wat zijn volgens jou kenmerkende eigenschappen of gedragingen?
8. Wat is de schade die slachtoffers oplopen en hoe groot is de impact van slachtofferschap volgens jou?
9. Op welke manier zoeken slachtoffers hulp? Weten ze waar ze terecht kunnen en waar hebben zij behoefte aan?
10. We willen bij ouderen bereiken dat ze zich bewust zijn van de risico's van aan- en ver koopfraude, dat het financiële gevolgen kan hebben en dat ze weten wanneer ze met een frauduleuze actie te maken hebben.
a. Als we dit willen bereiken, waar moeten we dan volgens jou rekening mee houden bij het ontwikkelen van een interventie?
b. Wat zijn volgens jou goede manieren om deze groep te benaderen?
c. Op welke wijze kan het gedrag van leden van de groep goed beïnvloed worden?
d. Waar zijn zij wel/ niet vatbaar voor?

3. PHISHING

4. Herken jij dat ouderen slachtoffer worden van phishing?
5. Hoe komt het volgens jou dat ouderen hier slachtoffer van worden? Wat zijn volgens jou kenmerkende eigenschappen of gedragingen?
6. Wat is de schade en de impact hiervan volgens jou voor de slachtoffers?
7. Op welke manier zoeken slachtoffers hulp? Weten ze waar ze terecht kunnen en waar is behoefte aan?
8. We willen bij ouderen bereiken dat ze zich bewust zijn van de risico's van phishing, hoe ze het kunnen herkennen en wat ze kunnen doen om slachtofferschap te voorkomen.
    a. Als we dit willen bereiken, waar moeten we dan volgens jou rekening mee houden bij het ontwikkelen van een interventie?
b. Wat zijn volgens jou goede manieren om deze groep te bereiken?
c. Op welke wijze kan het gedrag van deze groep goed beïnvloed worden?
d. Waar zijn zij wel/niet vatbaar voor?

Jongeren vragenlijst

Doel

- verifiëren van de uitkomsten van het lopende onderzoek bij lokale partijen. Klopt het beeld per doelgroep (jongeren, ouderen, mkb'ers) voor wat betreft de cyberdelicten waar zij slachtoffer van worden?
- Het vaststellen van de do's en don'ts bij het aanspreken of bereiken van de doelgroep

Algemene info:

- Naam organisatie + functie gesprekspartner:_____
- Relatie tot de doelgroep:_____

1. SEXTORTION

11. Herken jij dat deze doelgroep slachtoffer wordt van sextortion?
12. Hoe komt het volgens jou dat in deze doelgroep slachtoffers vallen? Wat zijn volgens jou kenmerkende eigenschappen of gedragingen?
13. Wat is de schade die slachtoffers oplopen en hoe groot is de impact van slachtofferschap volgens jou?
14. Op welke manier zoeken slachtoffers hulp? Weten ze waar ze terecht kunnen en waar hebben zij behoefte aan?
15. We willen bij jongeren bereiken dat ze zich bewust zijn van de risico's van sextortion (dat het strafbaar is, dat het risico's met zich meebrengt en dat het verstrekkende gevol gen kan hebben voor hun toekomst).
    a. Als we dit willen bereiken, waar moeten we dan volgens jou rekening mee houden bij het ontwikkelen van een interventie?
    b. Wat zijn volgens jou goede manieren om deze groep te benaderen?
    c. Op welke wijze kan het gedrag van leden van de groep goed beïnvloed worden?
    d. Waar zijn zij wel/ niet vatbaar voor?

2. HACKING

11. Herken jij dat jongeren slachtoffer worden van hacking?
12. Hoe komt het volgens jou dat in deze doelgroep slachtoffers vallen? Wat zijn volgens jou kenmerkende eigenschappen of gedragingen?
13. Wat is de schade die slachtoffers oplopen en hoe groot is de impact van slachtofferschap volgens jou?
14. Op welke manier zoeken slachtoffers hulp? Weten ze waar ze terecht kunnen en waar hebben zij behoefte aan?
15. We willen bij jongeren bereiken dat ze zich bewust zijn van de risico's van hacking en dat ze zichzelf beter beschermen hiertegen.
    a. Als we dit willen bereiken, waar moeten we dan volgens jou rekening mee houden bij het ontwikkelen van een interventie?
    b. Wat zijn volgens jou goede manieren om deze groep te benaderen?
    c. Op welke wijze kan het gedrag van leden van de groep goed beïnvloed worden?
    d. Waar zijn zij wel/ niet vatbaar voor?

3. Money muling

9. Herken jij dat jongeren zich schuldig maken aan money muling?
10. Hoe komt het volgens jou dat jongeren zich hieraan schuldig maken? Wat zijn volgens jou kenmerkende eigenschappen of gedragingen?
11. Wat is de schade en de impact hiervan volgens jou voor de daders?
12. We willen bij jongeren bereiken dat ze zich bewust zijn van de risico's van money muling (dat het strafbaar is, dat het risico's met zich meebrengt en dat het verstrekkende gevolgen kan hebben voor hun toekomst).

a. Als we dit willen bereiken, waar moeten we dan volgens jou rekening mee houden bij het ontwikkelen van een interventie?
b. Wat zijn volgens jou goede manieren om deze groep te bereiken?
c. Op welke wijze kan het gedrag van deze groep goed beïnvloed worden?
d. Waar zijn zij wel/niet vatbaar voor?